UNIVERSITÉ MOHAMMED V – AGDAL
FACULTÉ DES SCIENCES
Rabat

N° d'ordre 2717

Thèse de Doctorat
Présentée par

Chouaib MOUJAHDI

Titre

Protection des systèmes de sécurité biométriques : contributions à la protection des modèles biométriques.

Discipline : Sciences de l'ingénieur
Spécialité : Informatique et Télécommunications

Soutenue le 28/06/2014, devant le jury composé de :

Président :

Driss ABOUTAJDINE	Professeur à la Faculté des Sciences de Rabat

Examinateurs :

Abdel Hakim Ameur EL IMRANI	Professeur à la Faculté des Sciences de Rabat
Rachid OULAD HAJ THAMI	Professeur à l'Ecole Nationale Supérieure d'Informatique et d'Analyse des Systèmes de Rabat
Ahmed HAMMOUCH	Professeur à l'Ecole Normale Supérieure de l'Enseignement Technique de Rabat
George BEBIS	Professeur à l'Université de Nevada – Reno, USA
Mohammed RZIZA	Professeur habilité à la Faculté des Sciences de Rabat

Invités :

Sanaa GHOUZALI	Professeure assistante à l'Université du Roi-Saoud, Riyad
Mounia MIKRAM	Professeur assistante à l'Ecole des Sciences de l'Information de Rabat

Faculté des Sciences, 4 Avenue Ibn Battouta B.P. 1014 RP, Rabat – Maroc
Tel +212 (0) 37 77 18 34/35/38, Fax : +212 (0) 37 77 42 61, http://www.fsr.ac.ma

Avant propos

Les travaux présentés dans ce mémoire ont été effectués au Laboratoire de Recherche en Informatique et Télécommunications (LRIT), à la Faculté des Sciences de Rabat, sous la direction du professeur Mohammed RZIZA et le co-encadrement de professeur Sanaa GHOUZALI et professeur Mounia MIKRAM.

Je remercie,tout d'abord, bien vivement aussi mon directeur de thèse, professeur Mohammed RZIZA (PH à la Faculté des Sciences de Rabat), pour sa confiance, sa disponibilité et son soutien continuel. Qu'il trouvent ici l'expression de ma gratitude pour ses précieux conseils et toute l'aide qu'il m'a procuré durant l'élaboration de ce travail.

Je remercie bien vivement aussi mon Professeur Sanaa GHOUZALI (PA at King Saud University, Ryiadh, Saudi Arabia), pour son encadrement, ses encouragements et aussi pour ses contributions qui m'ont permit de réaliser ce travail.

Je remercie bien vivement aussi mon Professeur Mounia MIKRAM (PA à l'École des Sciences de l'Information, Rabat), pour son encadrement, ses encouragements et aussi pour ses contributions qui m'ont permit de réaliser ce travail.

Je remercie bien vivement aussi mon Professeur Driss ABOUTAJDINE (PES à la Faculté des Sciences de Rabat) pour sa confiance, sa disponibilité et son soutien continuel. Qu'il trouvent ici l'expression de ma gratitude pour ses précieux conseils et toute l'aide qu'il m'a procurée durant l'élaboration de ce travail. Je le remercier également de m'avoir fait l'honneur d'être le président de ma soutenance.

Je remercie vivement le professeur Abdel Hakim Ameur EL IMRANI (PES à la Faculté des Sciences de Rabat), d'avoir accepté de juger mon travail, de s'être penché avec rigueur et grand intérêt sur ce rapport et de m'avoir fait l'honneur d'en être un rapporteur.

Je remercie vivement le professeur Rachid OULAD HAJ THAMI (PES à l'École Nationale Supérieure d'Informatique et d'Analyse des Systèmes), d'avoir accepté de juger mon travail, de s'être penché avec rigueur et grand intérêt sur ce rapport et de m'avoir fait l'honneur d'en être un rapporteur.

Je remercie vivement le professeur Ahmed HAMMOUCH (PES à l'École Normale Supérieure de l'Enseignement Technique de Rabat), d'avoir accepté de juger mon travail, de s'être penché avec rigueur et grand intérêt sur ce rapport et de m'avoir fait l'honneur d'en être un rapporteur.

Je remercie bien vivement aussi mon Professeur George BEBIS (Professor and Chair at University of Nevada Reno, USA), premièrement de m'avoir invité à visiter le laboratoire *Computer Vision Laboratory* pour travailler ensemble sur les problèmes traités dans cette thèse, et deuxièmement de m'avoir fait l'honneur d'en être un examinateur.

Je n'oublie pas non plus de remercier la commission MACECE (Moroccan-American Commission for Educational and Cultural Exchange) de m'avoir sélectionné pour participer au programme "Joint Supervision Doctoral Grant".

J'aime remercier aussi Monsieur Omar MOUJAHDI et Madame Ilham BENMALLOUK qui m'ont aidé à vérifier et optimiser la langue de ce rapport.

Enfin, je voudrais remercier ma famille, en particulier ma mère et mon père, qui m'a donné l'éducation sans laquelle je n'en serais pas là aujourd'hui.

Protection des systèmes de sécurité biométriques : contributions à la protection des modèles biométriques

Résumé : Bien que les systèmes de sécurité biométriques aient des avantages inhérents par rapport aux systèmes traditionnels d'authentification personnelle qui utilisent les mots de passe et les cartes ID, le problème d'assurer la sécurité et la confidentialité des données biométriques demeure critique. L'utilisation croissante de la biométrie dans la conception des systèmes de sécurité a provoqué un regain d'intérêt pour la recherche et l'exploration de nouvelles méthodes servant à attaquer les systèmes biométriques. Ces recherches ont prouvé que la biométrie a donné lieu à de nouveaux problèmes et défis liés à la sécurité des données personnelles. Problèmes qui sont encore plus compliqués que ceux des systèmes traditionnels.

Les modèles biométriques, stockés dans la base de données, présentent une préoccupation majeure pour la sécurité et la vie privée des systèmes d'authentification biométriques. D'une part, en raison de la liaison forte entre le modèle d'un utilisateur et son identité ; et d'autre part, pour la nature irrévocable de ces modèles. Nous croyons que l'évaluation des menaces liées aux attaques contre les modèles biométriques et le développement des schémas de protection de ces modèles, sont le bon chemin qui mène à une technologie biométrique plus robuste et plus sécurisée. C'est la perspective suivie dans cette thèse.

Dans ce contexte, nous avons proposé deux nouvelles approches pour la protection des modèles biométriques. Une première approche, appelée Spiral Cube, pour la protection des modèles biométriques représentés sous forme de vecteurs ; et une deuxième approche, appelée Fingerprint Shell, pour la protection des systèmes de reconnaissance des empreintes digitales qui utilisent des modèles biométriques sous forme de points d'intérêt. Bien que les nouvelles approches fournissent toutes les exigences d'un schéma de protection idéal, elles sont suffisamment robustes contre les attaques à force brute et les attaques à zéro effort.

Mots-clefs : Biométrie, Modèle biométrique, Révocabilité, Diversité, Sécurité.

Biometric security protection : contributions to biometric template protection

Abstract : Although biometric systems have inherent advantages over traditional systems of personal authentication which use passwords and ID cards, the problem of ensuring the security and privacy of biometric data is critical. The increasing use of biometrics in the design of secure systems has led to a renewed interest in the research and exploration of new tricks to attack biometric systems. These researches showed that personal authentication systems based on biometrics have given rise to new problems and challenges related to the protection of personal data, issues which are of less importance in traditional authentication systems.

The attacks against the biometric templates, which are stored in the database module, can be considered the most damaging attacks on a biometric system ; because of the strong link between a user's template and his/her identity ; and also because of the irreversibility of biometric templates. We believe that the evaluation of threats related to attacks against biometric templates and the design of biometric template protection schemes is the right path to build a more robust and secure biometric technology. This is the followed perspective in this thesis.

In this context, we have proposed two new approaches for biometric template protection. First, Spiral Cube protection approach which is applicable to any biometric system that employs feature vectors for classification. Second, Fingerprint Shell approach which is designed for fingerprint recognition systems that use minutiae-based representation. The new approaches provide all the requirements of a perfect protection scheme. Moreover, they are sufficiently robust to the zero effort and brute force attacks.

Keywords : Biometrics, Biometric template, Revocability, Diversity, Security.

Table des matières

1 Introduction **5**

1.1 Biométrie et sécurité 5
1.2 Objectifs et contributions 13
1.3 Organisation du rapport 14

2 Sécurité des systèmes biométriques **17**

2.1 Introduction 17
2.2 Menaces générales contre les applications de sécurité 18
2.3 Sécurité, intégrité et vie privée d'un système biométrique 20
2.4 Échec intrinsèque d'un système biométrique 23
2.5 Niveaux d'attaque sur un système biométrique 24
2.5.1 Attaques directes sur l'interface utilisateur 25
2.5.2 Attaques sur l'interface entre les modules 27
2.5.3 Attaques sur les modules logiciels 30
2.5.4 Attaques contre la base de données 32
2.6 Pourquoi la protection des modèles biométriques ? 34
2.7 Exigences à respecter par un schéma de protection 35
2.8 Résumé du chapitre et conclusions 36

3 État de l'art de la protection des modèles biométriques **37**

3.1 Introduction 37
3.2 Solutions palliatives 39
3.3 Solutions préventives 40
3.3.1 Approches matérielles des solutions préventives 41
3.3.2 Transformation de caractéristiques 43
3.3.3 Crypto-systèmes biométriques 51
3.3.4 Approches hybrides 55
3.4 Résumé du chapitre et conclusions 56

4 Évaluation de performance et de sécurité des schémas de protection **57**

4.1 Introduction 57
4.2 Evaluation de performances 58
4.2.1 Convivialité des systèmes biométriques 59
4.2.2 Protocole FVC 62
4.3 Évaluation de sécurité 64

4.3.1 Vulnérabilité aux attaques d'intrusion 65
4.3.2 Vulnérabilité à la liaison de bases de données 66
4.4 Résumé du chapitre et conclusions 67

5 Nouvelles approches de protection des modèles biométriques 69
5.1 Introduction 69
5.2 Spiral Cube pour la protection des modèles biométriques 70
5.2.1 Introduction 70
5.2.2 Suite logistique 71
5.2.3 Spiral Cube 74
5.2.4 Expérimentations et discussion 77
5.2.4.1 Bases de données et procédures d'experimentation 77
5.2.4.2 Évaluation en utilisant la base de données YALE 80
5.2.4.3 Évaluation en utilisant la base de données PolyU FKP . . 85
5.2.4.4 Évaluation en utilisant la base de données CASIA 89
5.2.4.5 Évaluation en utilisant la base de données UMIST 92
5.2.4.6 Performance avec des modèles de grandes tailles 95
5.3 Fingerprint Shell pour la protection des minuties 96
5.3.1 Introduction 96
5.3.2 Reconnaissance des empreintes digitales 98
5.3.3 Travaux connexes 100
5.3.4 Fingerprint Shell 102
5.3.5 Expérimentations et discussion 105
5.4 Résumé du chapitre et conclusions 110

6 Conclusion générale et perspective 113

7 Résumé étendu en arabe 115

A Annexes 127
A.1 L'algorithme Hill-Climbing 127
A.2 Orthogonalisation de Gram-Schmidt 127
A.3 Régénération d'un modèle protégé par BioPhasor 128
A.4 Laplacian Smoothing Transform (LST) 128
A.5 Algorithme de construction d'une courbe F.S 129

Bibliographie 131

Table des figures

1.1 Niveaux d'attaque dans un système biométrique. 9

2.1 Exemples de traits biométriques falsifiés. 26
2.2 Images faciales résultantes d'une attaque hill-climbing après plusieurs itérations (prises de [Adler 2003]). F) L'image cible d'un utilisateur légitime. A) L'image initiale choisie aléatoirement pour débuter l'attaque. B) Après 200 itérations. C) Après 500 itérations. D) Après 3200 itérations. E) Après 4000 itérations. 29
2.3 Procédure d'attaque contre le module d'extraction de caractéristiques en utilisant un programme de type Cheval de Troie et une algorithme de type hill-climbing. 31
2.4 Exemple de la régénération des empreintes digitales à partir des minuties (prise de [Galbally *et al.* 2010]). La grande image à gauche est l'image originale. Les six petites images sont des images générées à partir des minuties extraites de l'image originale. 33

3.1 Catégorisation des approches de protection des systèmes biométriques. . . . 38
3.2 Exemples des technologies Match-on-Card et System-on-a-Chip. 41
3.3 Architecture et fonctionnement de Match-on-Card et System-on-a-Chip. . . 42
3.4 Mécanisme général d'authentification d'un système de sécurité biométrique protégé par une approche de transformation de caractéristiques. 44
3.5 Protection des modèles biométriques en utilisant le régime Biohashing. . . 45
3.6 Exemples de transformations géométriques appliquées sur le visage et les minuties des empreintes digitales (images prises de [Nagar *et al.* 2010, Campisi 2013, Rane *et al.* 2013]). 49
3.7 Mécanisme général d'authentification des crypto-systèmes biométriques de type key-binding et key generation [Jain *et al.* 2008]. 52

4.1 Exemples des courbes FAR, FRR, DET, ROC et le point EER. 61
4.2 Exemple d'un histogramme de distribution des scores légitime / imposteur. 63
4.3 Exemples des courbes IRIS et IRID. 66
4.4 Exemples des courbes CMR_o et CMR_t. 67

5.1 Implémentation de la suite logistique dans l'environnement Matlab. 72
5.2 Construction de Spiral Cube. 73
5.3 Mécanisme de construction des matrices de projection. 75

5.4 Exemples des images de la base de données Yale. 77
5.5 Exemples des images de la base de données PolyU FKP. 78
5.6 a) Image d'iris de la base CASIA b) détection d'iris c) segmentation d) normalisation. Images générées en utilisant [Masek & Kovesi 2003] 79
5.7 Exemples des images de la base de données SHEFFIELD. 79
5.8 Courbes ROC en utilisant la base de données YALE. 81
5.9 Courbes IRIS en utilisant la base de données YALE. 82
5.10 Courbes IRID en utilisant la base de données YALE. 82
5.11 Courbes CMR_o en utilisant la base de données YALE. 83
5.12 Courbes CMR_t en utilisant la base de données YALE. 83
5.13 Courbes ROC en utilisant la base de données PolyU FKP. 85
5.14 Courbes IRIS en utilisant la base de données PolyU FKP. 86
5.15 Courbes IRID en utilisant la base de données PolyU FKP. 86
5.16 Courbes CMR_o en utilisant la base de données PolyU FKP. 87
5.17 Courbes CMR_t en utilisant la base de données PolyU FKP. 88
5.18 Courbes ROC en utilisant la base de données CASIA. 89
5.19 Courbes IRIS en utilisant la base de données CASIA. 90
5.20 Courbes IRID en utilisant la base de données CASIA. 90
5.21 Courbes CMR_o en utilisant la base de données CASIA. 91
5.22 Courbes CMR_t en utilisant la base de données CASIA. 91
5.23 Taux d'échec de l'attaque proposée. 93
5.24 Illustration des résultats des régimes de protection. 94
5.25 Fonctionnement général d'un système de reconnaissance des empreintes digitales basé sur l'utilisation des minuties. 99
5.26 Exemple de l'implémentation de la méthode de comparaison proposée dans [Kryszczuk *et al.* 2004]. 99
5.27 Exemples de translation et rotation de deux impressions d'un même doigt (images prises de [Jain *et al.* 2008, Uz *et al.* 2009]). 101
5.28 Exemple de deux points singuliers. 103
5.29 Procédure générale de la construction de Fingerprint Shell. 104
5.30 Illustration de la révocabilité / diversité ; exemple de deux impressions de la même identité en utilisant deux différentes d_0. 105
5.31 Histogramme de deux systèmes protégés par Fingerprint Shell en utilisant FVC2002 DB1. 107
5.32 Histogramme du système 1 et pseudo-légitimes distributions en utilisant les systèmes 2 et 3. 108
5.33 Courbes ROC dans le scénario d'attaque à zéro effort en utilisant FVC2002 DB1 et DB2. 109

Liste des tableaux

5.1 Critères de convivialité / efficacité en utilisant la base YALE. 84
5.2 Critères de convivialité / efficacité en utilisant la base PolyU FKP. 88
5.3 Critères de convivialité / efficacité en utilisant la base CASIA. 92
5.4 Critères de convivialité / efficacité en utilisant des modèles biométriques de différentes tailles. 96
5.5 Précision de vérification basée sur le protocole FVC (valeurs en %) 108
5.6 Précision de la vérification de Fingerprint Shell dans le scénario d'attaque à zéro effort (valeurs en %) 110

CHAPITRE 1

Introduction

Sommaire

1.1 Biométrie et sécurité 5
1.2 Objectifs et contributions 13
1.3 Organisation du rapport 14

Tout d'abord, il est important de se rappeler que la sécurité absolue n'existe pas. Étant donné le financement, les bonnes circonstances, la technologie appropriée et le temps, presque tout système de sécurité peut être rompu.

Cependant, cela ne veut pas dire que le concepteur de tel système ne devrait pas faire son mieux pour se prémunir contre toutes les menaces possibles de sécurité. L'objectif de la communauté de sécurité doit être la protection et le développement des ressources, nécessaires à un attaquant, pour l'empêcher de compromettre la sécurité.

Dans ce contexte, on peut dire qu'il n'existe pas une sécurité générique, parce que le type de sécurité nécessaire dépend des exigences du système. Autrement dit, la notion de sécurité se change selon le type du système visé.

Le but de ce chapitre est de définir notre position exacte dans ce domaine large de la recherche en sécurité afin de clarifier le contexte de ce travail et la perspective suivie lors de l'élaboration de la thèse.

1.1 Biométrie et sécurité

Avec la croissance exponentielle des communications, tant en volume qu'en diversité (déplacement physique, transaction financière, accès aux services, etc.), les préoccupations internationales ont fait ressortir ces nécessités en vue de lutter contre les problèmes du

vol d'identité, la fraude, le crime et le terrorisme. Nous pouvons définir le vol d'identité comme l'utilisation abusive ou non autorisée d'une information personnelle volée (i.e., mot de passe, carte ID, empreinte digitale, etc.) pour profiter d'un service ou pour le saboter, ou une combinaison de ces types d'abus. Par exemple, dans le dernier rapport du ministère de la justice américain [1], le nombre moyen des victimes du vol d'identité aux États-Unis chaque année est de 11 571 900 et la perte financière totale attribuée à ce problème en 2013 est de 21 billions de dollars (elle a été de 13.2 billions de dollars en 2010). Ce qui donne une image claire sur les grandes menaces de ce problème sur plusieurs niveaux.

Face à ces responsabilités politiques, d'une part, et à ce besoin de protection civile d'autre part, les systèmes d'identification et d'authentification de personnes connaissent un intérêt grandissant et suscitent un vif intérêt dans différents domaines, tels que le secteur bancaire, les services publics, ainsi que dans le domaine de transport et notamment celui de voyages. Leur dénominateur commun, est d'offrir des moyens simples, pratiques, fiables, pour vérifier l'identité d'une personne, sans l'assistance d'une autre personne. Ces systèmes d'authentification doivent authentifier les personnes avec précision, avec célérité, d'une manière fiable, d'une manière conviviale, à moindre coût, sans envahir la vie privée des utilisateurs et sans changements drastiques aux infrastructures existantes.

Les systèmes traditionnels d'authentification personnelle qui font usage des mots de passe ou des cartes d'identité ne sont pas en mesure de répondre à toutes ces exigences. Par exemple, la plupart des gens utilisent des mots de passe basés sur des lettres ou des nombres qu'ils peuvent se rappeler facilement, comme les noms, les dates d'anniversaires et les personnalités connues ou la musique préférée. En effet, cela rend ces mots de passe faciles à deviner en utilisant une attaque à force brute ou une attaque par dictionnaire. En outre, bien qu'il est conseillé d'utiliser des mots de passe différents pour des applications différentes, la plupart des gens utilisent le même mot de passe sur différentes applications. Si un seul mot de passe est compromis, toutes les applications seront menacées. En pratique, les mots de passe, qui sont aléatoires et longs, sont plus sécurisés, mais ils sont plus difficiles à retenir, ce qui incite certains utilisateurs à les écrire dans des endroits accessibles (par exemple, un

1. U.S. Department of Justice, Javelin Strategy & Research, June 18th 2013

fichier texte ou un papier).

Par contre, les systèmes d'authentification basés sur la biométrie qui utilisent des propriétés physiologiques (visage, empreintes digitales, etc.) et comportementales (signature, voix, etc.) ont prouvé une priorité par rapport aux systèmes traditionnels. Le but d'un système biométrique est de simuler le système de reconnaissance humain par la machine pour automatiser certaines applications telles que : la carte d'identité nationale, le permis de conduire, la sécurité sociale, le contrôle des frontières, le contrôle des passeports, la télésurveillance, le contrôle d'accès à des sites, l'accès à des bâtiments sécurisés, les sciences cognitives, la recherche criminelle et l'identification de terroriste, etc.

Les différents moyens biométriques présentent l'avantage, par rapport aux systèmes traditionnels, qu'ils sont universels, uniques, permanents et plus fiables, puisque l'information biométrique ne peut pas être perdue, oubliée (il a été rapporté que près de 25% de tous les appels au service d'assistance des systèmes traditionnels sont liés aux mots de passe oubliés), ou devinée facilement. Pourtant, bien que la biométrie peut améliorer la sécurité dans une multitude d'environnements, les systèmes biométriques, comme tout autre système de sécurité, ont des vulnérabilités et points faibles.

L'utilisation croissante de la biométrie pour la conception des systèmes de sécurité a provoqué un regain d'intérêt dans la recherche et l'exploration de nouvelles méthodes pour attaquer les systèmes biométriques. Ces recherches ont prouvé que le recours à la biométrie a donné lieu à de nouveaux problèmes et défis liés à la sécurité et la protection des données personnelles. Ces nouveaux problèmes sont encore plus compliqués que ceux des systèmes traditionnels. Nous pouvons les résumer brièvement comme suit [Ratha *et al.* 2006] :

- *la biométrie ne fournit pas le secret* : bien que les caractéristiques biométriques assurent l'unicité, elles ne fournissent pas le secret. En effet, la biométrie utilise des modalités (visage, iris, empreintes digitales, signature, voix, etc.) qui peuvent être imitées ou prises sans conscience ou consentement. Par exemple, chaque personne a ses propres empreintes digitales (unicité), mais cette personne laisse ses empreintes sur n'importe quelle surface touchée (non secret). Dans ce contexte, nous pouvons

dire que l'information biométrique n'est pas secrète, ce qui rend le problème d'assurer la sécurité et la confidentialité des données biométriques très critique.

- *La biométrie ne fournit pas la révocabilité* : chaque individu est défini dans un système biométrique par un modèle de caractéristiques. Si ce modèle est volé, la sécurité du système sera gravement menacée, car, contrairement à un mot de passe ou une carte d'identité, il n'est pas possible pour un utilisateur légitime de révoquer ses modèles biométriques et les remplacer par un autre ensemble d'identificateurs. Cela peut aussi empêcher l'utilisateur du ré-enrôlement au système.

- *La biométrie a des utilisations secondaires* : les applications biométriques sont conçues spécifiquement pour les problèmes de sécurité, mais elles peuvent être utilisées très différemment dans d'autres environnements. Par exemple, le permis de conduire est conçu pour prouver l'identité et la légitimité de conduire à un agent de police, mais il peut être utilisé autrement pour prouver l'âge, le nom et même la citoyenneté dans d'autres environnements. Un autre aspect de ce problème est la violation de la vie privée. Si une personne utilise la même modalité biométrique dans plusieurs applications, elle peut être suivie facilement dans certaines situations, ce qui peut présenter une violation critique de sa vie privée.

Ces problèmes rendent les systèmes de sécurité biométriques souffrir de plusieurs vulnérabilités qu'on peut diviser en deux catégories principales. Premièrement, vulnérabilités à des attaques qui peuvent affecter n'importe quelle application de sécurité [Ferguson *et al.* 2010]. Puisque les systèmes biométriques sont mis en œuvre généralement sur des serveurs, il est évident alors qu'ils sont vulnérables à tout type d'attaques qui menacent les systèmes informatiques modernes comme les virus et les logiciels malveillants. Deuxièmement, vulnérabilités à des attaques développées spécifiquement contre les systèmes biométriques, qu'on peut diviser également en deux catégories : les attaques à zéro-effort et les échecs en raison d'une attaque adverse.

L'attaque à zéro-effort (appelée aussi *échec intrinsèque*) est la défaillance de la sécurité en raison d'une décision erronée faite par le système biométrique. Un système peut faire

deux types d'erreurs dans la prise de décision : les faux rejets et les fausses acceptations. Les faux rejets sont causés par les variations intra-sujet qui peuvent être dues à l'interaction incorrecte de l'utilisateur avec le système biométrique (changement de la pose de visage par exemple), ou par le bruit introduit au niveau du capteur (résidus de traces laissées sur un capteur d'empreintes digitales). Les fausses acceptations sont causées par le manque de l'individualité ou l'unicité de la caractéristique biométrique qui peut conduire à une forte similitude entre les ensembles de modèles des différents utilisateurs (la similitude dans les images de jumeaux ou frères et sœurs). Les fausses acceptations constituent une menace grave si leurs probabilités sont élevées. Pour limiter les effets des échecs intrinsèques, on peut soit développer des capteurs plus fiables ou utiliser la biométrie multimodale (l'utilisation de plusieurs traits biométriques dans le même système biométrique).

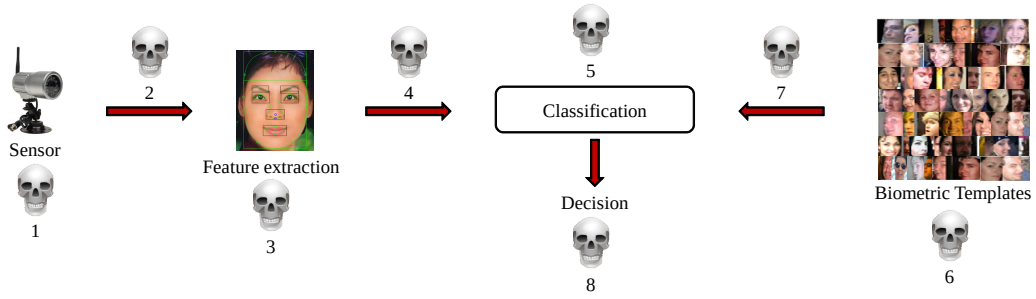


FIGURE 1.1 – Niveaux d'attaque dans un système biométrique.

Pour les échecs en raison d'une attaque adverse. Généralement, Les adversaires exploitent la structure des systèmes biométriques pour lancer des attaques spécifiques à un ou plusieurs modules / interfaces. Tous les systèmes biométriques sont composés de quatre modules principaux (Figure1.1) : le module du capteur qui est utilisé pour détecter les données biométriques provenant d'un utilisateur. Le module de l'extraction de caractéristiques qui est responsable de sélectionner les caractéristiques les plus significatives dans une image envoyée par le capteur pour construire un modèle biométrique de test. Le module de la base de données qui contient les modèles biométriques des utilisateurs légitimes, et enfin le module de comparaison ou de classification qui permet de comparer les modèles de test avec les modèles stockés dans la base de données pour prendre une décision finale.

Cette architecture donne lieu à plusieurs types d'attaques. En littérature, les vulnérabilités et les attaques contre un système biométrique ont été présentées sous plusieurs formes / modèles et à partir de plusieurs points de vue [2] [Ratha *et al.* 2001, Ratha *et al.* 2003, Cukic & Bartlow 2005, Adler 2005, Jain *et al.* 2006, Roberts 2007, Jain *et al.* 2008]. Nous présentons ici le modèle de [Ratha *et al.* 2001]. Les auteurs ont identifié huit niveaux d'attaque dans un système biométrique (Figure1.1). Nous pouvons les résumer comme suit :

1. L'attaque à ce niveau consiste à présenter une fausse donnée biométrique sur le capteur (iris falsifié, masque, etc.). Cette attaque est appelée *spoofing* si la modalité utilisée est de nature physiologique et *mimicry* si elle est comportementales.
2. A ce niveau, des données biométriques interceptées sont soumises au module de l'extraction de caractéristiques en passant le capteur. Le canal, entre le capteur et le module de l'extraction de caractéristiques, peut être intercepté pour voler une image (selon la modalité biométrique utilisée) d'un utilisateur légitime prise par le capteur. Cette image peut être rejouée ultérieurement au module d'extraction de caractéristiques en contournant le capteur.
3. Le module de l'extraction de caractéristique est remplacé par un programme *Cheval de Troie* (Trojan-horse) qui fonctionne selon les spécifications de son concepteur.
4. Le canal entre le module de l'extraction de caractéristiques et de classifieur peut être espionné par un adversaire pour enregistrer un modèle biométrique d'un utilisateur légitime. Ce modèle peut être rejoué ultérieurement sur le même canal.
5. Un programme de type cheval de Troie peut se déguiser en un classifieur, en contournant le vrai module de comparaison, pour soumettre un score de correspondance qui permet de prendre une décision qui est en faveur de l'adversaire.
6. L'attaque à ce niveau est contre les modèles biométriques stockés (voler, remplacer, supprimer ou modifier les modèles). Cette attaque pourrait être lancée au cours du temps d'enrôlement, pendant la période de vérification, ou à tout moment directement sur la base de données. Dans une application de carte à puce, où le modèle est

2. INCITS, Study Report on Biometrics in E-Authentication, https ://standards.incits.org/kwspub/home/

stocké dans la carte qui est portée par l'utilisateur, si la carte est perdue ou volée, et si elle n'est pas protégée d'une manière adéquate, le modèle biométrique peut être récupéré facilement.

7. A ce niveau, les modèles biométriques sont trafiqués dans le support de transmission entre la base de données et le classifieur et ils peuvent être rejoués ultérieurement sur le même canal.

8. Le canal entre le classifieur et l'application qui a envoyé une requête de vérification, peut être espionné pour accéder à la réponse d'une vérification précédente et l'enregistrer. Cette réponse peut être rejouée ultérieurement dans le même canal.

Chacune de ces attaques dépend d'une chaîne de ressources et d'exigences, ce qui rend la sévérité et la gravité varier d'une attaque à une autre. L'attaque au niveau 6, contre les modèles biométriques stockés dans la base de données (serveur) du système, peut être considérée comme une préoccupation majeure pour la communauté de la sécurité et l'une des attaques les plus dommageables contre un système biométrique ; d'une part en raison de la liaison forte entre les modèles d'un utilisateur et son identité, et d'autre part en raison de la nature irrévocable des modèles biométriques. En outre, elle est liée d'une manière ou d'une autre à toutes les autres attaques. L'utilisation de la cryptographie classique (symétriques comme AES ou à clé publique comme RSA) pour sécuriser les modèles biométriques n'est pas appropriée pour plusieurs raisons : 1) il est impossible de réaliser la comparaison dans le domaine de chiffrement, car le cryptage n'est pas une fonction lisse et une petite différence dans les valeurs des ensembles de caractéristiques extraites des données biométriques brutes (qui est toujours le cas en pratique), conduirait à une très grande différence dans les caractéristiques cryptées résultantes ; 2) le décryptage des modèles biométriques à chaque tentative d'authentification / identification rendra les modèles vulnérables aux attaques d'écoutes ; 3) La sécurité de ces systèmes dépend totalement de la sécurité de la clé cryptographique.

Nous croyons, comme beaucoup d'autres études et recommandations [ISO/IEC 2011], que l'évaluation des menaces liées à l'attaque au niveau 6 et le développement des schémas

de protection des modèles biométriques, sont le bon chemin qui mène à une technologie biométrique plus robuste et plus sécurisée. C'est la perspective suivie dans cette thèse.

Dans le passé proche, l'intérêt de la recherche en biométrie a été orienté notamment vers la précision, la rapidité, le coût et la robustesse. Mais ce n'est que récemment, quelques attentions ont été versées à des questions de la sécurité et la confidentialité des systèmes biométriques. Pourquoi devrons-nous faire confiance à la technologie biométrique ? Comment pouvons-nous la sécuriser ? Qui assure le niveau de sécurité offert par un système biométrique ? Que faire si mes données biométriques ont été volées ou détournées ? Ces questions et autres questions similaires sont devenues urgentes et ayant besoin de réponses satisfaisantes.

Pour répondre à ces questions et résoudre ces problèmes, plusieurs initiatives, académiques [3] [4] [5], commerciales [6] [7] et gouvernementales [8] [9], ont essayé de développer de nouveaux régimes de protection des systèmes biométriques, y compris des techniques de la protection des modèles biométriques. Chacune de ces solutions disponibles a ses propres avantages / inconvénients, mais elles ne sont pas encore suffisamment matures pour le déploiement à grande échelle ; elles ne répondent pas, simultanément, à toutes les exigences nécessaires (révocabilité, diversité, sécurité et performance). En dépit de cela, les systèmes biométriques sont encore déployés pour sécuriser les frontières internationales, le contrôle d'accès et pour éliminer le vol d'identité !

Le concept de la biométrie *révocable* (appelé *revocable* or *cancelable* en anglais) a été proposé, pour la première fois, comme une solution pour sécuriser des modèles biométriques par [Ratha *et al.* 2001]. La révocabilité signifie que nous pouvons révoquer un modèle compromis et le remplacer par un autre modèle, de la même façon qu'un mot de passe volé peut être remplacé par un nouveau. La plupart des approches de protection des modèles biométriques sont basées sur ce concept. Dans cette thèse, nous sommes plus in-

3. Biometric Template Security Project, http ://biometrics.cse.msu.edu/projects/
4. Security of approaches to personnel authentication, http ://www.nislab.no/research/projects/hig10037
5. Biometrics Revisited for Security, Confidence and Dependability, http ://atvs.ii.uam.es/listprojects.do
6. Securics Inc., Colorado Springs, CO, http ://www.securics.com/
7. Precise Biometrics, Sweden, http ://www.precisebiometrics.com/
8. TURBINE (TrUsted Revocable Biometric IdeNtitiEs), http ://www.turbine-project.eu/
9. TABULA RASA (Trusted Biometrics under Spoofing Attacks), http ://www.tabularasa-euproject.org/

téressés à ce genre de solutions.

Le défi majeur dans la conception d'un régime de protection des modèles biométriques (qui répond à toutes les exigences) est la nécessité de gérer les variations intra-sujet (qui diffèrent d'une modalité à une autre), parce qu'en pratique, de multiples acquisitions de la même caractéristique (trait) biométrique ne conduisent pas à un ensemble de caractéristiques identiques, ce qui rend ces régimes de protection incapables de fournir la sécurité et la performance simultanément. La plupart de ces solutions échangent la sécurité pour la performance ou l'inverse. En outre, la conception des approches génériques de protection des modèles biométriques est entravée aussi par le type de la représentation de ces modèles. Ces derniers sont stockés dans la plupart des systèmes biométriques sous forme de vecteurs de caractéristiques. Cependant, ils sont utilisés sous forme de points d'intérêt dans autres systèmes (par exemple, la représentation sous forme de minuties dans les systèmes de la reconnaissance des empreintes digitales), ce qui nécessite la conception des approches de protections spécifiques. En bref, la protection des modèles biométriques représente un problème critique et un défi ouvert qui suscite des efforts de recherche intensifs.

1.2 Objectifs et contributions

Les principaux objectifs de la thèse sont les suivants : 1) étudier le problème de la sécurité des systèmes biométriques afin d'identifier et d'évaluer les menaces et les attaques possibles en mettant notamment l'accent sur celles liées aux modèles biométriques ; 2) analyser et étendre l'état de l'art actuel de la protection des modèles biométriques ; 3) développer de nouvelles approches génériques de la protection des modèles biométriques afin d'améliorer la robustesse des systèmes biométriques contre les attaques possibles, et cela sans procéder à un changement drastique sur la structure du système à protéger ; 4) évaluer les méthodes proposées en utilisant des protocoles de test efficaces et des bases de données largement disponibles pour la communauté de la recherche en biométrie.

Les principales contributions de cette thèse résident dans : 1) la conception d'une nouvelle approche basée sur la projection aléatoire, appelée *Spiral Cube*, pour la protection des

modèles biométriques (représentés sous forme de vecteurs), qui répond aux exigences de la révocabilité, la diversité, la sécurité et la performance. Une analyse de sécurité rigoureuse et des expériences approfondies sont élaborées pour évaluer l'approche proposée. Nous avons comparé spiral Cube avec deux autres schémas de protection qui sont basés aussi sur la projection aléatoire. 2) La conception d'une nouvelle approche pour la protection des systèmes de la reconnaissance des empreintes digitales. Nous avons proposé une nouvelle représentation, appelée *Fingerprint Shell*, qui peut être utilisée au lieu de la représentation traditionnelle basée sur les minuties. Bien que la nouvelle approche répond à toutes les exigences, sa performance est moins sensible à la translation / rotation des empreintes digitales (par rapport aux systèmes traditionnels) et elle est suffisamment robuste contre les attaques à force brute et les attaques à zéro effort.

1.3 Organisation du rapport

Le présent manuscrit s'articule, outre la conclusion générale, autour de cinq parties essentielles, présentées de la manière suivante :

- Le chapitre 1 introduit le problème de la sécurité dans les systèmes biométriques, clarifie le contexte de ce travail et la perspective suivie lors de l'élaboration de la thèse et précise les objectifs et les principales contributions.
- Afin de poser correctement les problématiques traitées dans ce rapport, le chapitre 2 est consacré à introduire les menaces générales contre les applications de sécurité ; à détailler les vulnérabilités des systèmes biométriques à un certain nombre d'attaques et à aborder les exigences d'un schéma idéal de protection des modèles biométriques.
- Le chapitre 3 contient une étude de l'état de l'art des travaux sur la protection des systèmes de sécurité biométriques en mettant l'accent sur les méthodes de la protection des modèles biométriques. Cet état de l'art présente un survol sur les principales méthodes utilisées pour résoudre le problème de la vulnérabilité des systèmes bio-

métriques. Cette étude dévoile les différentes techniques proposées au sein de la communauté de recherche en soulignant les limites et les avantages de chacune.

- Le chapitre 4 aborde les différentes méthodologies statistiques d'évaluation de performance et de sécurité des systèmes biométriques qui seront utilisées ultérieurement dans notre expérimentation. Des méthodologies d'évaluation spécifiques aux schémas de protection des modèles biométriques sont également présentées.
- Le chapitre 5 présente deux nouvelles approches de protection des modèles biométriques proposées dans le cadre de cette thèse ; l'évaluation expérimentale de chaque approche est présentée également. Ces méthodes sont : 1) *Spiral Cube* pour la protection des modèles biométriques. 2) *Fingerprint Shell* pour la protection des empreintes digitales.
- Le chapitre 6 conclut le mémoire en résumant les principaux résultats obtenus ; il expose également les perspectives et les travaux futurs.
- Chapitre 7 présente un résumé étendu en arabe de la thèse.

CHAPITRE 2

Sécurité des systèmes biométriques

Sommaire

2.1 Introduction 17
2.2 Menaces générales contre les applications de sécurité 18
2.3 Sécurité, intégrité et vie privée d'un système biométrique 20
2.4 Échec intrinsèque d'un système biométrique 23
2.5 Niveaux d'attaque sur un système biométrique 24
2.5.1 Attaques directes sur l'interface utilisateur 25
2.5.2 Attaques sur l'interface entre les modules 27
2.5.3 Attaques sur les modules logiciels 30
2.5.4 Attaques contre la base de données 32
2.6 Pourquoi la protection des modèles biométriques ? 34
2.7 Exigences à respecter par un schéma de protection 35
2.8 Résumé du chapitre et conclusions 36

2.1 Introduction

Bien que les systèmes de sécurité biométriques aient des avantages inhérents par rapport aux systèmes traditionnels d'authentification personnelle, le problème d'assurer la sécurité et la confidentialité des données biométriques demeure critique. L'utilisation croissante de la biométrie dans les applications de la sécurité a provoqué un regain d'intérêt pour la recherche et l'exploration de nouvelles méthodes pour attaquer les systèmes biométriques. Ces recherches ont prouvé que ces systèmes sont vulnérables à un certain nombre d'attaques. Le but principal de ce chapitre n'est pas d'aborder une étude exhaustive des publications existantes traitant les attaques possibles qui peuvent être lancées contre un système biométrique ; mais plutôt de présenter une vue générale en portant une attention particulière aux attaques contre les modèles biométriques.

Dans ce chapitre, dans un premier temps, nous allons présenter les menaces générales contre les applications de sécurité (section 2.2) et clarifier les notions de la sécurité, l'intégrité et la vie privée dans le contexte des systèmes biométriques (section 2.3). Ensuite, nous allons détailler les types d'attaques qui peuvent être lancées contre un système biométrique (section 2.5) et les modes d'échecs de ce dernier (section 2.4). Dans la section 2.6, nous allons montrer l'importance de la protection des modèles biométriques dans le processus de la construction d'une technologie biométrique plus robuste / sécurisée. Nous abordons les exigences d'un schéma idéal de protection des modèles biométriques dans la section 2.7. Enfin, le résumé du chapitre et les conclusions sont présentés dans la (section 2.8).

2.2 Menaces générales contre les applications de sécurité

Les systèmes biométriques font partie des systèmes de sécurité qui sont encore plus larges et qui ont des architectures différentes et plus compliquées. Il faut ainsi, comme première étape, comprendre les menaces de sécurité dans le contexte de ces systèmes larges. En pratique, pour être capable de décider si une solution de sécurité est adéquate et efficace, il est très important de définir clairement les menaces possibles contre le système à protéger. Ces dernières se diffèrent selon l'environnent et la nature du système. Cependant, nous pouvons définir un modèle de menaces générales qui est adéquat pour toutes les applications de sécurité. Les menaces générales contre une application de sécurité peuvent inclure les éléments suivants [Maltoni *et al.* 2003, Ferguson *et al.* 2010] :

- *Déni de service* (Denial of service (DoS) en anglais) : l'attaquant essaye d'endommager le système de sorte qu'il ne peut plus être consulté par les utilisateurs légaux. Il peut prendre plusieurs formes ; ralentissement ou arrêt du système (par exemple via une surcharge de requêtes dans le réseau) ou dégradation de performance (par exemple via l'intrusion de plusieurs échantillons bruyants qui peuvent pousser le système à diminuer automatiquement son seuil de décision et d'accroître ainsi le taux de fausses acceptations FAR). DoS peut être utilisée pour l'extorsion du propriétaire du système ou pour des raisons politiques.

- *Contournement* : c'est le cas de l'attaque où un utilisateur non autorisé accède au système. Cette attaque peut être lancée pour deux raisons : l'espionnage ou le sabotage. Dans le cas de l'espionnage, l'attaquant obtient l'accès aux données privées des utilisateurs légitimes. Dans le cas du sabotage, un adversaire peut accéder au système pour des objectifs subversifs. Par exemple, il peut accéder au compte bancaire d'une personne pour retirer son argent.

- *Répudiation* : dans ce type de menace, l'utilisateur légitime nie l'accès au système. Par exemple, dans une application bancaire, un utilisateur légitime peut d'abord bénéficier d'un service, il nie plus tard son profit et il le reçoit à nouveau (ce scénario est appelé en anglais *double jobbing* ou *double dipping*).

- *Contamination* (*contamination* ou *covert acquisition* en anglais) : c'est le cas d'une attaque directe où l'adversaire utilise des informations d'authentification, capturées à partir d'un utilisateur légitime, pour accéder au système. Par exemple, enregistrer et rejouer les mots de passe vocaux et aussi la conception des parodies physiques à partir des empreintes digitales reconstruites.

- *Collusion* : Dans toute application de sécurité, certains utilisateurs du système auront un statut *spécial* qui leur permet de contourner le système et sa décision (par exemple, un administrateur du système ou une personne qui n'a pas les doigts et qui est légitime dans un système de reconnaissance des empreintes digitales). Cette propriété est intégrée dans le workflow des systèmes de sécurité pour manipuler les situations exceptionnelles. Cependant, cela pourrait conduire à un abus du système par le biais d'une collusion entre les utilisateurs *spéciaux* et les adversaires. Le proverbe sacré des hackers est comme suit : "*la meilleure façon pour rompre un système de sécurité est de contourner l'administrateur du système*".

- *Coercition* : dans ce cas, l'utilisateur légitime peut être forcé ou obligé à aider l'attaquant pour accéder au système. Par exemple, un utilisateur d'une ATM pourrait être contraint à donner sa carte de guichet automatique et aussi son mot de passe à une personne armée.

Il faut noter que, selon l'architecture de chaque système de sécurité, certaines de ces attaques peuvent être possibles dans un système, mais pas dans un autre. Dans les sections suivantes, nous allons détailler les menaces les plus pertinentes aux systèmes biométriques et aussi les notions de sécurité, intégrité et vie privée dans le contexte de ces applications de sécurité biométriques.

2.3 Sécurité, intégrité et vie privée d'un système biométrique

Il convient de noter que, même si plusieurs notions sont traitées séparément dans cette section, elles sont interdépendantes à bien des égards. Par conséquent, cette discussion a tendance à se chevaucher dans certaines parties.

La biométrie est considérée, dans le contexte des systèmes d'authentification personnelle, comme une approche relativement nouvelle et différente ; en raison de la nature différente des données biométriques et de son mode d'emploi dans ce type de systèmes. En littérature, il y a un consensus que la biométrie fournit l'unicité car l'information biométrique est plus étroitement liée à une personne en particulier, et cela est considéré comme un atout majeur de la technologie. Cependant, au cours des dernières années, un certain nombre de critiques ont été adressées à la biométrie par la communauté de recherche en sécurité. Critiques qui sont la plupart du temps corrects, tandis que d'autres ne sont pas totalement valides ; d'une part, parce que ces critiques sont basées sur une incompréhension fondamentale de la technologie biométrique elle-même ; et d'autre part, parce que la sécurité des systèmes biométrique a été analysée dans un paradigme traditionnel à laquelle ils n'appartiennent pas. La plupart des systèmes d'authentification traditionnels ou cryptographiques sont généralement basés sur le secret d'une clef (mot de passe, carte ID, clé cryptographique, etc.). Cependant, la plupart des données biométriques ne sont pas considérées comme des secrets, ainsi elles ne relèvent pas du paradigme traditionnel.

Puisque la plupart des données biométriques ne sont pas dans le moule traditionnel, il faut confirmer que la biométrie présente certainement une révolution scientifique. Par conséquent, il est nécessaire de définir la notion de sécurité dans le nouvel contexte exigé

par cette nouvelle technologie. Selon [Jain *et al.* 2007], puisque la biométrie est le processus de la reconnaissance des personnes en utilisant ses caractéristiques comportementales et/ou physiologiques, nous pouvons considérer la vulnérabilité ou le manque de sécurité dans un système biométrique comme le résultat d'une reconnaissance inexacte et/ou incorrecte, soit en raison d'un échec intrinsèque ou d'une attaque directe/indirecte ou de n'importe quelle menace citée dans la section précédente 2.2. Par conséquent, dans ce contexte, la sécurité d'un système biométrique peut être définie tout simplement par son absence.

Nous avons déjà mentionné que la biométrie ne fournit pas le secret, parce que les données biométriques ne sont pas secrètes. Alors la question évidente qui se pose est comme suit : si les systèmes biométriques ne peuvent pas compter sur le secret / confidentialité de leurs données, sur quoi faut-il compter ? La réponse est l'intégrité des données biométriques [INCITS 2006]. Dans les systèmes traditionnels, le principal mécanisme pour protéger le secret de toutes les données se fait via le cryptage. Mais ce dernier n'est pas toujours approprié dans le cas des systèmes biométriques pour certaines raisons : 1) il est impossible de réaliser la comparaison des modèles biométriques dans le domaine de chiffrement, car le cryptage n'est pas une fonction lisse et une petite différence dans les valeurs des ensembles de caractéristiques extraites à partir des données biométriques brutes conduirait à une très grande différence dans les caractéristiques cryptées résultantes ; 2) le décryptage des modèles biométriques, à chaque tentative d'authentification, rendra les modèles originaux vulnérables aux écoutes ; 3) en utilisant cette manière, la sécurité des systèmes biométriques dépend totalement de la sécurité de la clé cryptographique. Par conséquent, dans le contexte de la biométrie, le secret des données biométriques ne fournit pas la protection et la sécurité aux systèmes biométriques, mais plutôt l'intégrité des données biométriques est le facteur critique le plus important.

L'intégrité d'un système biométrique est essentielle pour assurer sa sécurité globale. Selon [Campisi 2013], l'intégrité est la capacité de rendre les ressources du système inchangées, modifiées ou manipulées. En pratique, l'intégrité d'un système biométrique dépend bien de la *protection* de ses *modèles biométriques* [Albrecht *et al.* 2003] (entre autres

procédures, *l'horodatage certifié* par exemple ; *timestamping* en anglais).

Il faut noter que la discussion des notions de secret et intégrité, dans le contexte de la biométrie, a divisé les points de vue des chercheurs, concernant la sécurité des systèmes biométriques, en deux philosophies : la sécurité par *obscurité* (*security through/by obscurity* en anglais) et la sécurité par *transparence* (*security through/by design* en anglais). En général, les systèmes qui reposent sur le principe de la sécurité par obscurité souffrent, d'un point de vue théorique et/ou pratique, de quelques failles de sécurité. Cependant, les supporters de ce principe confirment qu'un attaquant ne sera pas en mesure de rompre le système si et seulement s'il connait ses failles ; et selon leur croyance, ce scenario est peu probable. De l'autre côté, la sécurité par transparence suit le *principe de Kerckhoffs* [Kerckhoffs 1883] reformulé par le mathématicien *Claude Shannon* [1] comme suit : "*l'adversaire connaît le système*". Alors dans les approches qui reposent sur le principe de la sécurité par transparence, le système doit être sécurisé, même si tout ce qui concerne le système, à l'exception d'une clef, est public. C'est le principe de base de tous les cryptosystèmes classiques. Cependant, il ne faut pas oublier que la biométrie est différente par rapport à la cryptographie, et elle ne peut pas être sécurisée de la même façon.

Nous croyons que les deux points de vue peuvent fournir un niveau de protection et que chaque philosophie ne peut pas annuler l'autre. Notre point de vue, concernant la sécurité biométrique, est de développer des schémas de protection qui fournit l'équilibre entre l'obscurité et la transparence. C'est la voie suivie dans cette thèse.

Pour la vie privée (*privacy* en anglais) des systèmes biométriques [Campisi 2013, Breebaart *et al.* 2009], elle n'est pas une question de sécurité en soi parce que nous pouvons avoir la sécurité sans vie privée, mais nous ne pouvons pas avoir une vie privée sans sécurité. Toutefois, elle est un facteur important qui influe certainement sur les décisions concernant le déploiement de la technologie biométrique, en particulier par les utilisateurs. La vie privée résume la capacité d'un utilisateur pour utiliser et contrôler son identité, sans être suivi, volé ou compromis, malgré que ses informations personnelles soient révélées lors de l'inscription, l'utilisation, le stockage, la modification, le transfert et la suppression.

1. http ://en.wikipedia.org/wiki/Claude_E._Shannon

La confidentialité des données biométriques doit être protégée pour assurer la vie privée, alors que les mécanismes de sécurité sont nécessaires pour assurer cette protection. En bref, dans le contexte des systèmes biométriques, la sécurité et l'intégrité des données biométriques garantissent la vie privée.

Les définitions et les points de vue, que nous avons abordés dans cette section, sont suivis dans le reste de cette thèse. Mais comme indiqué au début de cette section, il faut noter que dans le contexte de la biométrie, les notions de la sécurité et l'intégrité interfèrent bien. Alors nous avons utilisé seulement le terme sécurité pour mentionner les deux notions dans le reste de la thèse.

2.4 Échec intrinsèque d'un système biométrique

L'erreur intrinsèque (appelée aussi l'attaque à zéro effort) [Jain *et al.* 2008] est la défaillance de la sécurité en raison d'une décision erronée faite par le système biométrique. Un système peut faire deux types d'erreurs dans la prise de décision : les faux rejets et les fausses acceptations.

Les faux rejets peuvent être causés par les variations intra-sujet, qui peuvent être dues à l'interaction incorrecte de l'utilisateur avec le système biométrique (i.e., changement de la pose de visage, rotation / translation d'une impression de doigt), ou par du bruit introduit au niveau du capteur (i.e., résidus de traces laissées sur un capteur d'empreintes digitales). Les fausses acceptations sont causées par le manque de l'individualité ou l'unicité de la caractéristique biométrique qui peut conduire à une forte similitude entre les ensembles de modèles de différents utilisateurs (i.e., la similitude dans les images de jumeaux ou frères et sœurs). Les fausses acceptations constituent une menace grave si ses probabilités sont élevées. L'erreur intrinsèque peut également être causée par l'utilisation des modules (i.e., module de sélection de caractéristiques, module de comparaison) inadéquats ou non-robustes.

Il est impossible d'empêcher cette attaque et elle est présente dans tous les systèmes biométriques. Cette attaque est dérivée du fait qu'il existe toujours une probabilité que

deux modèles biométriques provenant de deux identités différentes sont suffisamment semblables pour produire un score qui permet l'accès au système (de la même façon qu'il y a toujours une probabilité de deviner par hasard un mot de passe dans un système traditionnel). Cette probabilité dépend principalement du trait biométrique utilisé et de la performance / précision du système [Pankanti *et al.* 2002, Jain *et al.* 2008].

Pour limiter les effets des échecs intrinsèques, on peut soit développer des capteurs plus fiables ou utiliser la biométrie multimodale (l'utilisation de plusieurs traits biométriques dans le même système biométrique).

Comme cette vulnérabilité est plus liée à la nature statistique et la conception des systèmes biométriques, la communauté de recherche en biométrique a mis l'accent sur l'étude des attaques adversaires. Nous allons détailler ces attaques dans la section suivante.

2.5 Niveaux d'attaque sur un système biométrique

En général, une attaque adversaire présente la possibilité qu'un adversaire (inscrit ou non inscrit dans le système) de contourner un système sans conscience de ses administrateurs / concepteurs. Les adversaires exploitent la structure des systèmes biométriques (Figure1.1) pour lancer des attaques spécifiques à un ou plusieurs modules / interfaces. En littérature, les vulnérabilités et les attaques contre un système biométrique ont été présentées sous plusieurs formes / modèles et à partir de plusieurs points de vue [Ratha *et al.* 2001, Ratha *et al.* 2003, Cukic & Bartlow 2005, Adler 2005, Jain *et al.* 2006, Roberts 2007, Jain *et al.* 2008]. [Ratha *et al.* 2001] ont identifié huit points ou niveaux d'attaque dans un système biométrique (voir 1.1). Toutefois, puisque le principe de certaines attaques se répète, [Jain *et al.* 2008] les ont regroupé en quatre catégories : 1) *attaques directes sur l'interface utilisateur* qui sont basées sur la présentation des données biométriques falsifiées au capteur du système [Schuckers 2002]. 2) *Attaques sur l'interface entre les modules* où l'adversaire peut détruire ou interférer les canaux de communication entre les modules du système [Syverson 1994, Adler 2004]. 3) *Attaques sur les modules logiciels* dans lesquelles le programme exécutable d'un module peut être modifié de sorte qu'il

retourne toujours les valeurs souhaitées par l'adversaire. Ceci est connu comme l'attaque Cheval de Troie (*Trojan-horse*[2] en anglais). 4) *Attaques contre les modèles biométriques* qui sont stockés dans la base de données du système. Les attaques de cette catégorie sont considérées parmi les attaques les plus dommageables à un système biométrique.

Dans les sous-sections suivantes (2.5.1, 2.5.2, 2.5.3 et 2.5.4), nous allons aborder chacune de ces catégories en citant les travaux les plus représentatifs liés à ces attaques.

2.5.1 Attaques directes sur l'interface utilisateur

Il existe plusieurs types d'attaques qui peuvent être lancées contre l'interface utilisateur (le capteur) d'un système biométrique. 1) Le capteur peut être physiquement détruit lors d'une attaque de type *déni de service*. 2) Un adversaire peut présenter des traits biométriques falsifiés (Figure 2.1) au système pour contourner le processus d'inscription ou de reconnaissance. Cette attaque est appelée *spoofing* si la modalité utilisée est de nature physiologique et *mimicry* si elle est comportementales. Plusieurs travaux, [Eriksson & Wretling 1997, Matsumoto *et al.* 2002, Lewis & Statham 2004, Geradts 2006, Alonso-Fernandez *et al.* 2009, Galbally *et al.* 2010], ont prouvé que les systèmes biométriques (basés sur la reconnaissance de visage, iris, empreintes digitales, géométrie de la main, veine, voix et signature) peuvent être trompés en présentant un trait synthétique ou une parodie physique au capteur.

La plupart des tests de susceptibilité d'un système biométrique à ce type d'attaque ont été exécutés sur les capteurs d'empreintes digitales, notamment parce que les capteurs commerciaux des empreintes sont facilement disponibles. Les méthodes connues de spoofing des empreintes digitales sont : 1) l'utilisation de prothèses créées à partir de moules prélevés d'un doigt légitime ; 2) l'utilisation d'une image de haute résolution d'une empreinte digitale inscrite ; 3) l'utilisation d'une membrane mince de silicone contenant une impression d'une empreinte digitale inscrite ; 4) l'utilisation des résidus des empreintes digitales laissées sur le capteur pour contourner le système ; 5) l'utilisation d'une moule 3D de gélatine d'une empreinte digitale. Pour les systèmes de reconnaissance de visage,

2. http ://en.wikipedia.org/wiki/Trojan_horse_(computing)

nous pouvons les contourner en présentant des images simples des utilisateurs légitimes pour le capteur, ou même des dessins très simples d'un visage humain. Une attaque encore plus sophistiquée, en utilisant un moniteur d'un téléphone portable ou une vidéo de visage, peut être lancée également. Pour les systèmes de reconnaissance de l'iris, ils peuvent être contournés en utilisant des lentilles artificielles contenant les caractéristiques d'un iris légitime ou une vidéo numérique. Dans les systèmes de la reconnaissance de signatures et voix, le mimicry est effectué au moyen d'imiter fidèlement la signature ou la voix d'un utilisateur légitime.

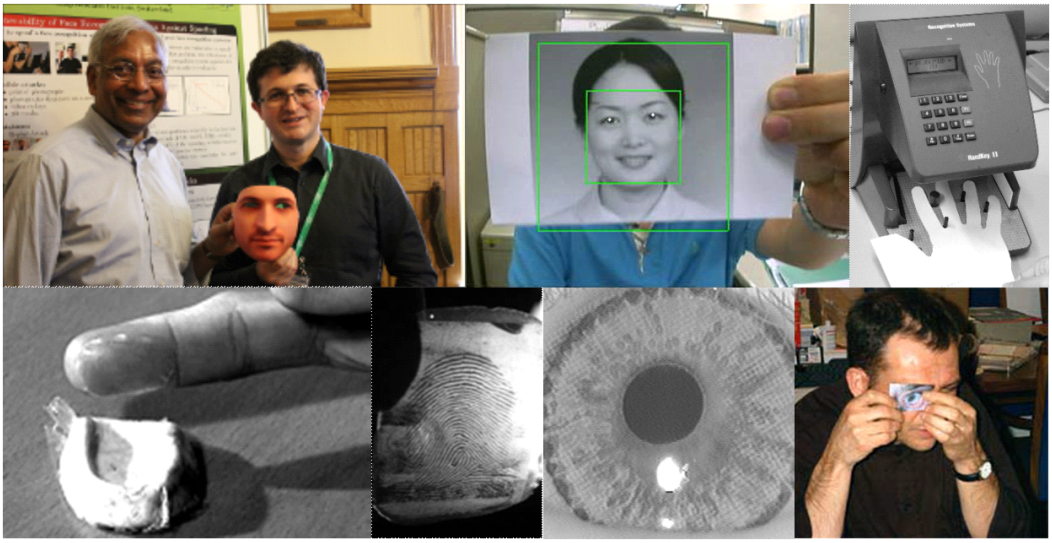


FIGURE 2.1 – Exemples de traits biométriques falsifiés.

Un certain nombre d'efforts ont été faits pour développer du matériel ainsi que des solutions logicielles pour détecter la vivacité d'identité au niveau du capteur (*liveness detection* en anglais) [Lee *et al.* 2005, Parthasaradhi *et al.* 2005, Antonelli *et al.* 2006, Galbally *et al.* 2009, Kim *et al.* 2013]. La détection de vivacité peut être mise en œuvre en utilisant trois méthodes : 1) ajouter des mesures physiques spécifiques au niveau du dispositif de capture (par exemple propriétés thermiques, optiques ou biomédicales) ; 2) ajouter des logiciels spécifiques dans le cadre du processus d'acquisition / traitement des images du capteur ; 3) combiner les techniques matérielles et logicielles.

Par exemple, pour les systèmes de reconnaissance des empreintes digitales, puisque

l'odeur de la peau est différente de l'odeur des matériaux des moules synthétiques comme la gélatine, latex et silicone ; des *capteurs chimiques* peuvent être utilisés [Franco & Maltoni 2008]. Ces capteurs détectent les substances odorantes en détectant les petites quantités de molécules qui sont évaporées à partir les matières de la parodie synthétique. Des propriétés optiques, comme l'absorption, la réflexion et autres, peuvent être utilisées également sous différentes conditions d'éclairage pour détecter la vivacité [Rowe *et al.* 2008]. Pour les systèmes de la reconnaissance faciale, ils peuvent demander à l'utilisateur d'effectuer un mouvement de la tête, un mouvement des lèvres, ou un changement dans l'expression du visage. Un système de la reconnaissance de signature peut demander à un utilisateur de répondre à un certain nombre de signatures de pré-inscription qui sont différentes de la signature permanente. Les systèmes de reconnaissance de la voix peuvent demander aux utilisateurs de réciter une phrase générée aléatoirement ou une séquence alphanumérique de manière à éviter les voix enregistrées ou la lecture numérique.

La résistance du système contre ce type d'attaques peut être levée également en utilisant l'authentification multi-facteurs (par exemple, un trait biométrique et un code PIN) ou en utilisant la biométrie multimodale (par exemple, le visage et la voix). Mais en général, contrairement au problème du vol / oubli des mots de passe dans les systèmes traditionnels qui est permanent ; nous croyons que ce type d'attaque sera limité avec le temps. Si une parodie physique peut tromper certains capteurs d'aujourd'hui, elle sera probablement détectée et rejetée facilement par les capteurs de demain vu l'amélioration drastique au niveau de la technologie et le matériel utilisés dans les nouveaux dispositifs de capture.

2.5.2 Attaques sur l'interface entre les modules

Les modules d'un système biométrique sont liés par des interfaces ou canaux de communication afin de transférer les informations nécessaires pour réaliser la tâche de reconnaissance (Figure 1.1). Plusieurs types d'attaques peuvent être lancés au niveau de ces interfaces : entre le capteur et l'extracteur de caractéristiques, entre l'extracteur de caractéristiques et le classifieur, entre la base de données et le classifieur, et entre le classifieur

et l'application de décision. Par exemple, un adversaire peut saboter ou empiéter les interfaces de communication entre les modules [Juels *et al.* 2005] (par exemple en plaçant un brouilleur près du canal). Un attaquant peut également intercepter et/ou modifier les données transférées dans les canaux [Syverson 1994, Adler 2005].

L'une des attaques les plus simples contre les canaux de communication d'un système biométrique est l'injection de données biométriques volées dans ces interfaces. En littérature, cette attaque est appelée *attaque par rejeu* (*replay attack* en anglais) [Syverson 1994]. Par exemple, un adversaire peut rejouer un modèle biométrique légitime obtenu précédemment par une écoute du canal pour accéder au système. La façon la plus courante pour sécuriser un canal est d'utiliser la cryptographie pour coder toutes les données envoyées en utilisant une infrastructure à clé publique [Schneier 1995]. La *signature numérique* (*digital signature* en anglais) ou *l'horodatage* (*timestamp* en anglais) peuvent être utilisés également pour assurer l'intégrité/sécurité des données transférées [Lam & Beth 1992]. Le mécanisme *challenge-réponse* est un autre alternatif pour éviter l'attaque par rejou [Bolle *et al.* 2002].

L'attaque *Hill-Climbing* est l'une des attaques les plus connues aussi dans cette catégorie, elle est introduite pour la première fois par [Soutar 2002]. En général, cette attaque exploite le score envoyé par le classifieur pour optimiser, d'une manière itérative, l'image biométrique utilisée par l'attaquant (ou un trait falsifié) jusqu'à ce que le score dépasse le seuil de décision pour garantir par conséquent l'accès au système (voir l'annexe A.1). Cette attaque peut être lancée dans plusieurs canaux du système. *Hill-Climbing* a prouvé son efficacité contre plusieurs modalités. Par exemple, [Adler 2003] a testé cette attaque dans les systèmes de la reconnaissance faciale (Figure 2.2) et [Uludag & Jain 2004] ont testé l'attaque dans le cas des empreintes digitales. Les résultats de ces travaux et ceux d'autres ont prouvé que les images calculées par hill-climbing sont d'une qualité suffisante pour contourner le système, et elles donnent de bonnes impressions visuelles qui sont très proches de celles des images légitimes.

Afin de prévenir cette attaque, plusieurs astuces peuvent être mises en œuvre : 1) il faut

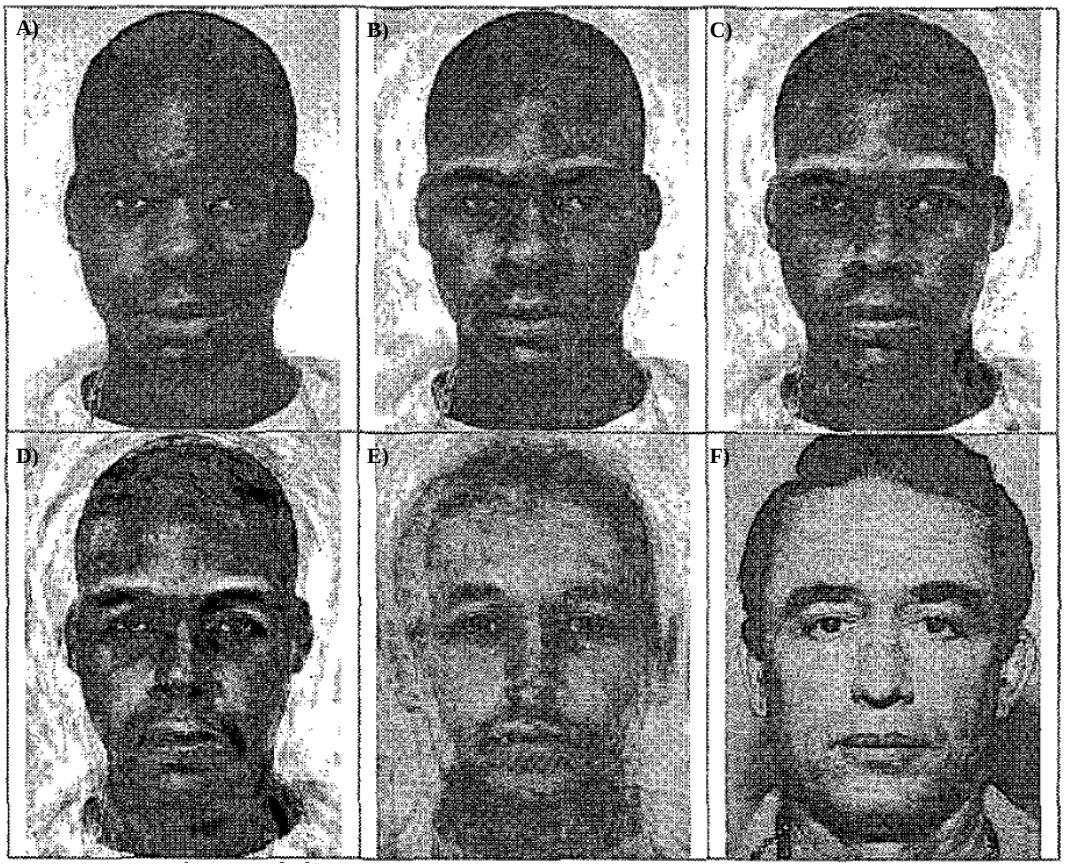


FIGURE 2.2 – Images faciales résultantes d'une attaque hill-climbing après plusieurs itérations (prises de [Adler 2003]). F) L'image cible d'un utilisateur légitime. A) L'image initiale choisie aléatoirement pour débuter l'attaque. B) Après 200 itérations. C) Après 500 itérations. D) Après 3200 itérations. E) Après 4000 itérations.

augmenter de la valeur du seuil de décision. 2) Il faut forcer le système à ne pas émettre les scores dans les canaux, seulement les décisions finales (match / non-match) peuvent être envoyées. 3) La quantification des scores peut être utilisée également pour contourner l'attaquant. 4) [Soutar 2002] a proposé aussi d'augmenter la granularité du score afin d'augmenter le nombre d'itérations de hill-climbing avant d'observer un changement dans le score résultant (image résultante également) de l'attaque. Par conséquent, le nombre total de tentatives nécessaires pour achever le score qui permet l'accès deviendrait très grand.

En pratique, l'attaque hill-climbing pourrait être très efficace seulement contre les systèmes de conception faible qui permettent de fournir les scores ou d'autres informations

qui pourraient être exploités pour lancer cette attaque. Cependant, hill-climbing peut être dangereuse même dans les systèmes, qui respectent cette règle générale de protection, en présence des programmes malveillants de type *Trojan horse* ; surtout au niveau du module de la sélection des caractéristiques.

2.5.3 Attaques sur les modules logiciels

Les attaques contre les modules logiciels du système est un autre type d'attaques potentielles dans le contexte des systèmes de sécurité biométriques ; où l'adversaire essaie d'émuler un des modules du système. Le programme exécutable sur un module peut être modifié ou remplacé de telle sorte qu'il retourne toujours les valeurs souhaitées par l'adversaire, c'est le principe de l'attaque *Cheval de Troie* (*Trojan-horse* en anglais). L'attaquant peut développer un programme pour imiter ou remplacer le module d'extraction de caractéristiques, le module de classification ou le module de la base de données.

Par exemple, au niveau du module de classification, si la fonction de comparaison ne gère pas correctement une valeur d'entrée spécifique X, cette vulnérabilité pourrait ne pas affecter le fonctionnement normal du système, car la probabilité que la valeur X étant générée à partir des données biométriques réelles peut être très négligeable. Mais un adversaire peut exploiter ainsi cette faille pour atteindre facilement la sécurité sans laisser de traces.

Au niveau du moule de l'extraction de caractéristiques, l'adversaire peut développer un algorithme de génération des images de test synthétiques qui ressemblent aux images du capteur utilisé. Ce programme peut ensuite envoyer les images au module de l'extraction de caractéristiques en passant le capteur. Le système peut être incapable de distinguer si les images proviennent de son capteur ou du logiciel malveillant de l'adversaire.

Comme nous avons mentionné dans la sous-section précédente 2.5.2, un programme de type Cheval de Troie peut être utilisé pour augmenter l'efficacité d'une attaque hill-climbing ; en évitant la procédure générale de protection qui consiste à bloquer le système après un certain nombre de fausses acceptations successives (Figure 2.3). Le même programme Trojan horse, décrit dans le paragraphe précèdent, peut être utilisé pour perturber

les requêtes du capteur comme première étape, ensuite il note et surveille le score du module de classification. Si le score est plus élevé que le score de l'itération précédente, les changements apportés à l'image d'entrée sont maintenus, sinon ils sont optimisés dans une autre itération du hill-climbing. Ainsi, à chaque itération, où le score est supérieur qu'avant, l'image d'entrée se rapproche d'être comme légitime. La procédure est répétée jusqu'à ce que le score soit supérieur au seuil. Alors Trojan-horse peut rendre hill-climbing encore plus efficace [Maltoni *et al.* 2003].

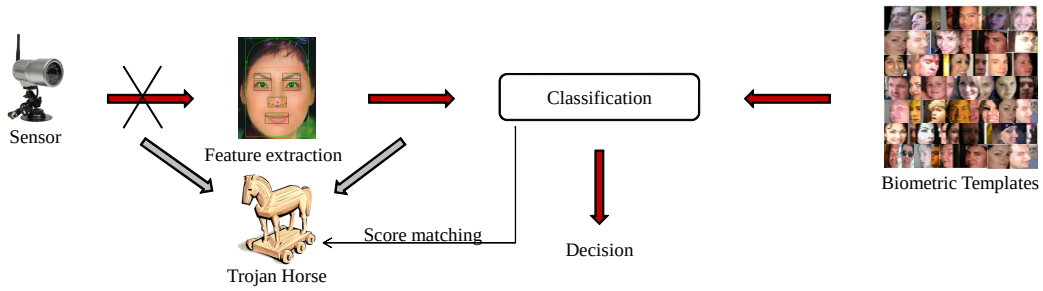


FIGURE 2.3 – Procédure d'attaque contre le module d'extraction de caractéristiques en utilisant un programme de type Cheval de Troie et une algorithme de type hill-climbing.

Il faut noter que l'adversaire peut utiliser plusieurs astuces pour livrer ses programmes de type Cheval de Troie. Par exemple, en utilisant les virus informatiques ou la technique de *hameçonnage* [3] (*Phishing* en anglais).

Les procédures possibles pour prévenir cette attaque diffèrent selon le type et le positionnement des modules de chaque système. Si tous les modules sont situés dans un même ordinateur (par exemple, un ordinateur personnel ou un téléphone mobile), les modules du système biométrique peuvent être protégés en utilisant un anti-virus. Si les modules du système sont distribués dans le contexte d'une application client-serveur, la stratégie des systèmes fermés [4] (*closed system* en anglais) devrait être appliquée. D'autres solutions ont été proposées [Cooper *et al.* 2007, Grother *et al.* 2009], surtout dans le contexte commercial et industriel, et qui se basent sur le principe de déplacement autant de modules que possible sur un matériel sécurisé (par exemple, une carte à puce). Ces techniques sont connues

3. http ://en.wikipedia.org/wiki/Phishing
4. http ://en.wikipedia.org/wiki/Closed_system#In_computing

par plusieurs noms : *Match-on-Card*, *System-on-Device* et *System-on-Card*. L'avantage de cette technologie est que les données biométriques ne quittent jamais la carte. Toutefois, cette technologie n'est pas appropriée pour la plupart des applications à grande échelle, car d'une part elle est coûteuse et les utilisateurs doivent porter leurs cartes avec eux tout le temps. D'autre part, car les modèles biométriques peuvent être récupérés facilement à partir d'une carte volée.

2.5.4 Attaques contre la base de données

Les modèles biométriques, stockés dans la base de données, présentent une préoccupation majeure pour la sécurité et la vie privée des systèmes d'authentification biométriques. D'une part, en raison de la liaison forte entre le modèle d'un utilisateur et son identité ; et d'autre part, parce qu'ils contiennent les informations biométriques les plus importantes.

Les attaques conte un modèle biométrique stocké peuvent prendre plusieurs formes : 1) le stockage peut être modifié (ajout, modification ou suppression des modèles) pour obtenir un accès non autorisé au système. Cette attaque pourrait être lancée au cours du temps d'enrôlement, pendant la période de vérification, ou à tout moment directement sur la base de données 2) Une parodie physique (spoof) peut être créée à partir d'un modèle volé [Adler 2004] pour obtenir un accès non autorisé au système (ainsi que dans d'autres systèmes qui utilisent le même trait biométrique). 3) Le modèle volé peut être rejoué devant le classifieur. 4) Un programme de type Cheval de Troie peut contourner la base de données du système pour soumettre des modèles biométriques volés ou générés artificiellement en passant le rôle de la base de données.

Nous pouvons dire que les trois catégories d'attaques (présentées dans 2.5.1, 2.5.2 et 2.5.3) sont liées d'une manière ou d'une autre aux attaques contre les modèles biométriques, ce qui rend la protection de ces modèles très importante pour assurer la sécurité générale du système (mais toujours entre autres procédures qui sont assez nécessaires). Autrement dit, si les modèles d'un système biométrique sont indignes de confiance, alors le processus d'authentification résultant du système sera indigne de confiance également.

Dans le passé proche, les fondateurs de l'industrie biométrique ont été totalement persuadés par le fait que la régénération des images originales des traits biométriques est irréalisable à partir des modèles biométriques [5] [6]. Ils ont étayé leurs affirmations par les arguments suivants [Jain *et al.* 2007] : 1) les modèles contiennent seulement les caractéristiques d'une image originale. 2) Les modèles sont généralement calculés en utilisant seulement une petite portion de l'image originale. 3) les modèles ont une très petite taille qui est beaucoup plus petite que la taille de l'image originale. Cependant, plusieurs études ont prouvé que la régénération des images biométriques originales est réalisable ; soit directement à partir des modèles biométriques [Ratha *et al.* 2006] (Figure 2.4) ou en utilisant les scores de correspondance [Adler 2003] (voir l'annexe A.1). Le chiffrement des modèles biométriques est nécessaire, mais il n'entrave pas totalement cette attaque ; parce que le décryptage des modèles à chaque tentative d'authentification est aussi nécessaire.

FIGURE 2.4 – Exemple de la régénération des empreintes digitales à partir des minuties (prise de [Galbally *et al.* 2010]). La grande image à gauche est l'image originale. Les six petites images sont des images générées à partir des minuties extraites de l'image originale.

Nous croyons, comme beaucoup d'autres études [Albrecht *et al.* 2003] et recommandations [ISO/IEC 2011] (ISO/IEC 24745 : *Information technology - Security techniques - Biometric template protection*), que le développement des schémas de protection des modèles biométriques, est le bon chemin qui mène à une technologie biométrique plus robuste

5. SecuGen (Page 8) : http ://www.secugen.com/download/SecuGenFingerprintReaderGuide.pdf
6. International Biometrics & Identification Association. http ://www.ibia.org/biometrics/faq/

et plus sécurisée. C'est la perspective suivie dans cette thèse.

2.6 Pourquoi la protection des modèles biométriques ?

En bref, il y a quatre raisons principales qui rendent la protection des modèles biométriques un challenge clef à résoudre pour améliorer la sécurité des systèmes biométriques :

1. Le problème de l'irrévocabilité des modèles biométriques. Dans les systèmes traditionnels, si un mot de passe est volé, il est facile de créer un nouveau mot de passe et de révoquer l'ancien de la base de données en créant une liste de révocation. Par contre, si un modèle biométrique est compromis par un attaquant, le modèle ne peut pas être changé (un trait biométrique est unique). Le développement des techniques de protection qui fournissent la révocabilité aux modèles biométriques est nécessaire.

2. Le problème de régénération des images originales à partir des modèles biométriques. C'est vrai que, contrairement à un mot de passe volé, il n'est pas trivial d'exploiter correctement un modèle biométrique volé par un adversaire non spécialisé, mais il ne faut pas supposer que l'adversaire est toujours non spécialisé. Les techniques de protection doivent garantir que l'adversaire ne peut pas récupérer l'information originale à partir du modèle volé.

3. Le problème de l'utilisation de la même modalité biométrique dans plusieurs systèmes de sécurité biométriques. Si un utilisateur est inscrit dans plusieurs systèmes avec le même trait biométrique, et si un de ses modèles est volé de l'un de ces systèmes ; tous les autres peuvent être compromis et l'utilisateur concerné peut être suivi partout. Autrement dit, l'absence de diversité entre les modèles du même trait biométrique menace la sécurité et la vie privée. Les techniques de protection doivent fournir la diversité aux modèles biométriques.

4. La liaison forte entre le vol d'un modèle biométrique et les différentes attaques possibles contre un système biométrique. La plupart du temps, pour lancer une attaque contre un système biométrique, un modèle volé est nécessaire. Les modèles protégés

(volés) ne doivent pas être utiles pour lancer autres types d'attaques.

Selon la norme ISO/IEC 24745 [ISO/IEC 2011] (sous-titre : *Biometric Template Protection*), il est recommandé de protéger les modèles biométriques en appliquant des transformations ou des distorsions sur les traits ou les modèles biométriques pour assurer la révocabilité. C'est le principe de base de la biométrie révocable [Ratha *et al.* 2001] utilisé par toutes les approches de la protection des modèles biométriques. Cette norme a détaillé les catégories de solutions de base, mais elle n'a pas favorisé aucune des techniques. ISO/IEC 24745 a abordé aussi les exigences à respecter par un schéma de protection des modèles biométriques, qu'on va présenter dans la section suivante.

2.7 Exigences à respecter par un schéma de protection

Une technique idéale de protection des modèles biométriques doit respecter les exigences suivantes [Jain *et al.* 2008, Breebaart *et al.* 2009, Campisi 2013] :

1. *La diversité* : les modèles biométriques protégés (qui appartiennent à la même identité inscrite dans plusieurs systèmes biométriques), ne devraient pas se correspondre pour éviter le *cross-matching* (suivi d'une personne dans plusieurs applications) et assurer la vie privée. Autrement dit, il devrait être possible de générer un grand nombre de modèles protégés (qui ne se correspondent pas) à partir d'un même modèle original non protégé pour que la personne sera capable d'utiliser le même trait biométrique dans différentes applications biométriques.

2. *La révocabilité* : il devrait être possible de révoquer un modèle biométrique compromis et générer un nouvel modèle qui est basé sur le même trait biométrique original (non protégé). La révocabilité est une conséquence directe de la diversité. Si une technique de protection fournit la diversité, il sera possible de générer de nouveaux modèles pour remplacer les anciens modèles menacés (qui seront enregistrés dans une *liste de révocation* [7]).

7. http ://en.wikipedia.org/wiki/Revocation_list

3. *La sécurité* : il doit être difficile, d'un point de vue calculatoire, de récupérer le modèle original à partir d'un modèle protégé. L'une des conséquences significatives de cette exigence est que la classification doit être effectuée dans l'espace des modèles protégés, ce qui peut dégrader considérablement la performance.
4. *La performance* : la technique de protection ne devrait pas dégrader, d'une manière drastique, les performances de la reconnaissance du système biométrique original. Si la performance est dégradée considérablement, les attaques à zéro effort deviennent encore plus faciles pour un adversaire qu'une attaque à force brute pour récupérer le modèle original.

Afin de protéger efficacement un modèle biométrique, ces quatre exigences doivent être respectées simultanément. La conception d'une technique de protection des modèles biométriques (qui respecte toutes les exigences) est un challenge très difficile en raison de la nécessité de gérer les variations intra-sujet (des multiples acquisitions du même trait biométrique ne conduisent pas à un ensemble de caractéristiques identiques). Ainsi, la protection des modèles est un sujet de recherche actif qui suscite des efforts de recherche tant en raison de ses applications potentielles que par le grand défi qu'elle présente.

2.8 Résumé du chapitre et conclusions

Dans ce chapitre, nous avons abordé la problématique traitée dans ce rapport. En effet, nous avons commencé par la description des menaces générales contre les applications de sécurité et par les notions de sécurité, intégrité et vie privée dans le contexte de la biométrie. Ensuite, nous avons mis l'accent sur les vulnérabilités et les attaques possibles contre un système biométrique en accordant une attention particulière aux attaques contre les modèles biométriques et à la perspective suivie dans cette thèse. Enfin, nous avons présenté les exigences à respecter par une technique de protection des systèmes biométriques.

Il faut noter que certaines parties et notions de ce chapitre sont basées sur quelques publications citées dans nos références. Cependant, la structure et l'exposition de ces parties sont présentées selon notre point de vue personnel.

CHAPITRE 3

État de l'art de la protection des modèles biométriques

Sommaire

3.1 Introduction 37
3.2 Solutions palliatives 39
3.3 Solutions préventives 40
3.3.1 Approches matérielles des solutions préventives 41
3.3.2 Transformation de caractéristiques 43
3.3.3 Crypto-systèmes biométriques 51
3.3.4 Approches hybrides 55
3.4 Résumé du chapitre et conclusions 56

3.1 Introduction

Dans ce chapitre, nous allons présenter une étude de l'état de l'art des travaux liés à la protection des systèmes de sécurité biométriques avec une attention particulière aux techniques de la protection des modèles biométriques. Ce chapitre dévoile les différentes techniques proposées au sein de la communauté de recherche en sécurité des systèmes biométriques ; en soulignant les limites et les avantages de chacune d'elle.

Nous pouvons diviser les solutions proposées en deux catégories principales (Figure 3.1) : solutions *palliatives* et solutions *préventives*. Chaque catégorie peut être divisée en deux types principaux : approches *matérielles* et approches *logicielles*. L'objectif des solutions palliatives est de distinguer entre un vrai trait humain et un trait artificiel ou falsifié, présentés au niveau du capteur. Les solutions préventives visent à éviter la perpétration d'une attaque. En général, ces solutions servent à protéger les modèles biométriques.

Dans cette thèse, nous sommes principalement concernés par les approches logicielles des solutions préventives qui visent la protection des modèles biométriques. Plus précisément, nous nous sommes plus intéressés aux approches de *transformation non inversible* ; d'une part, parce qu'elles sont les plus proches à nos objectifs dans cette thèse (section 1.2) ; et d'autre part, car nos approches proposées dans la thèse (*Spiral Cube* et *Fingerprint Shell*) sont des approches de transformation non inversible.

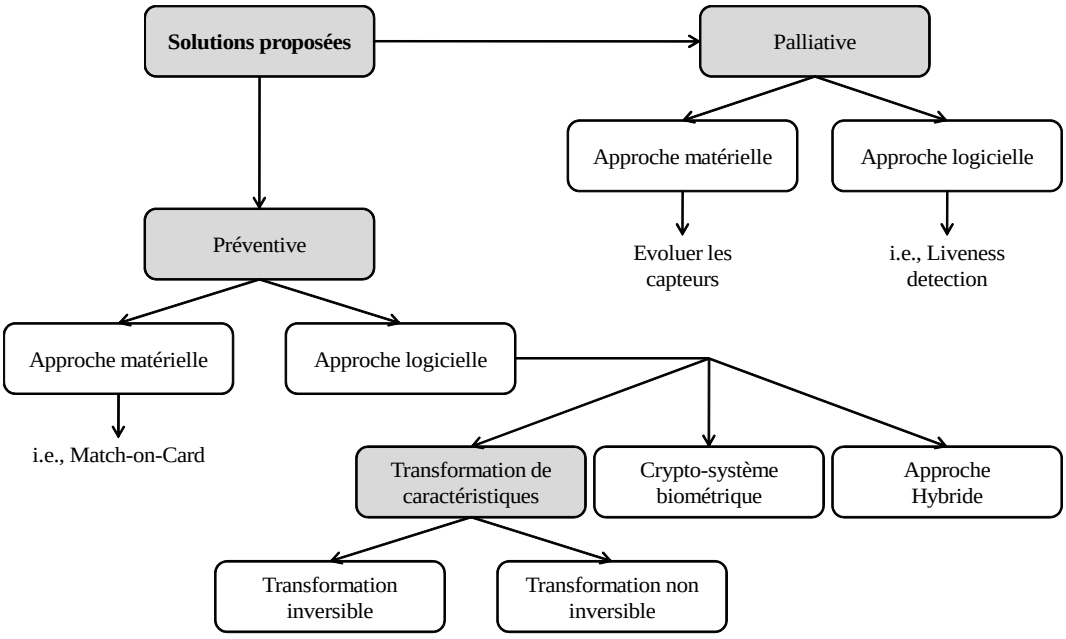


FIGURE 3.1 – Catégorisation des approches de protection des systèmes biométriques.

Le but principal de ce chapitre n'est pas d'aborder une étude exhaustive de toutes les publications existantes pour la protection des modèles biométriques ; mais plutôt notre objectif est de présenter une vue générale sur ces approches avec une attention particulière aux techniques de transformation de caractéristiques.

Dans ce chapitre, dans un premier temps, nous allons présenter brièvement les solutions palliatives (section 3.2). Ensuite, dans la section 3.3, nous allons détailler les approches préventives en concentrant notre étude sur les approches de transformations de caractéristiques les plus significatives (sous-section 3.3.2). Enfin, le résumé du chapitre et les conclusions sont présentés dans la section 3.4.

3.2 Solutions palliatives

Généralement, les solutions palliatives sont conçues pour éviter les attaques directes contre les capteurs des systèmes biométriques (voir sous-section 2.5.1). L'objectif principal de cette catégorie de solutions est de distinguer entre les vrais traits humains et les traits falsifiés, présentés par un adversaire directement sur l'interface utilisateur (le capteur) ; pour minimiser les probabilités de rupture dans le système. Ces techniques sont connues aussi par les notations anglaises : *liveness detection* ou *spoof detection*.

Pour les approches matérielles de ces solutions, elles consistent à ajouter des dispositifs spécifiques (par exemple, propriétés thermiques ou biomédicales) aux capteurs pour détecter la vivacité / fraude des traits biométriques présentés. Par exemple, [Lapslay *et al.* 1998] ont proposé un capteur biométrique des empreintes digitales qui peut déterminer si la pression artérielle (du flux sanguin) d'un trait biométrique présenté est compatible avec celle de l'humain. [Baldisserra *et al.* 2005] ont proposé un capteur évolué basé sur l'utilisation de l'odeur de la peau pour détecter la vivacité des empreintes digitales. Ce capteur et autres [Franco & Maltoni 2008], détectent les substances odorantes en détectant les petites quantités de molécules qui sont évaporées à partir des matières d'une empreinte falsifiée. [Pacut & Czajka 2006] ont proposé un capteur évolué pour les systèmes de la reconnaissance de l'iris, qui utilise la *contraction de la pupille* [1] (appelée *hippus* ou *pupillary athetosis* en anglais) pour détecter les iris falsifiés. Cette technique exploite la sensibilité de la pupille (qui est le trou situé au milieu de l'iris) au changement d'illumination ; car la fonction d'une pupille est de réguler l'intensité de lumière entrant dans l'œil en stimulant des mouvements involontaires des muscles de l'iris. Ces mouvements sont absents ou très limités dans le cas si un adversaire met un iris falsifié dans son œil.

Pour les approches logicielles des solutions palliatives, elles utilisent les caractéristiques extraites à partir des images envoyées du trait biométrique par le capteur et non à partir du trait lui-même comme dans les approches matérielles. Alors des logiciels spécifiques peuvent être utilisés dans le cadre du processus d'acquisition / traitement des

1. http ://en.wikipedia.org/wiki/Hippus

images du capteur pour détecter la vivacité des traits biométriques. Par exemple, les travaux [Tai *et al.* 2006, Yau *et al.* 2007, Cheng & Larin 2007, Rowe *et al.* 2008] utilisent les propriétés optiques (comme l'absorption, la réflexion et réfraction) de la peau humaine pour détecter la vivacité des empreintes digitales. La peau humaine a des propriétés optiques, différentes de celles des matériaux synthétiques utilisés dans les empreintes falsifiés, qui peuvent être exploitées pour détecter la vivacité des traits présentés. Les travaux [Moon *et al.* 2005, Choi *et al.* 2007, Tan & Schuckers 2008] ont proposé d'exploiter les images de très haute résolution de certains capteurs des empreintes digitales pour extraire certaines propriétés très fines de la peau, comme la position et la forme des pores, qui peuvent être utilisées pour la détection de la vivacité car il est difficile de créer des traits falsifiés qui contiennent ces propriétés avec une grande précision. Autres approches logicielles des solutions palliatives pour les systèmes de la reconnaissance du visage sont détaillées dans [Pan *et al.* 2008, Sun *et al.* 2011]. La méthode [Galbally *et al.* 2012] est un exemple d'anti-spoofing logiciel pour les systèmes de la reconnaissance d'iris et les travaux [Guo *et al.* 2001, Fierrez & Ortega-Garcia 2008] sont des techniques d'anti-spoofing comportementales qui sont destinées à la détection des signatures imitées.

Il faut noter que pour cette catégorie de solutions, il n'y a pas une approche standard pour tous les systèmes biométriques et sa conception dépend principalement de la modalité utilisée. Il faut noter aussi que les approches logicielles sont plus avantagées que les approches matérielles parce qu'elles coûtent beaucoup moins cher dans les applications réelles puisqu'aucun dispositif supplémentaire n'est nécessaire. Cependant, la combinaison des techniques matérielles avec les techniques logicielles est toujours la façon la plus efficace pour résister mieux aux attaques directes contre l'interface utilisateur.

3.3 Solutions préventives

En général, les solutions préventives essaient de protéger les modèles biométriques stockés dans la base de données du système. Cette catégorie de solutions a comme objectif de résoudre le problème de l'irrévocabilité des modèles biométriques. Les approches maté-

rielles des solutions préventives consistent à mettre tous les modules et les interfaces d'un système biométrique sur une carte à puce ou un processeur sécurisé en général (voir la sous-section 3.3.1). Les approches logicielles des solutions préventives sont conçues pour protéger les modèles biométriques stockés dans la base de données du système. L'idée de base de ces approches est qu'au lieu de stocker les modèles eux-mêmes, une fonction (ou transformation) de chaque modèle est stockée. Le modèle transformé (protégé) sera utilisé directement dans la tâche de classification. Nous pouvons classer ces approches logicielles en trois catégories (Figure 3.1) [Jain *et al.* 2008, Rathgeb & Uhl 2011] : 1) approches de transformation de caractéristiques (voir sous-section 3.3.2) ; 2) crypto-systèmes biométriques (voir sous-section 3.3.3) ; 3) approches hybrides (voir sous-section 3.3.4).

3.3.1 Approches matérielles des solutions préventives

L'objectif des approches matérielles des solutions préventives est de déplacer autant de modules (du système biométrique) que possible sur un matériel sécurisé (par exemple, une carte à puce qui possède une RAM, ROM, mémoire de stockage et un simple système d'exploitation ; Figure 3.2) pour s'assurer que les modèles biométriques ne quittent jamais ce matériel sécurisé et éviter les attaques d'intrusion [Bolle *et al.* 2002, Cooper *et al.* 2007]. Cette technologie utilise des processeurs spéciaux qui peuvent effectuer des opérations cryptographiques simples. Nous pouvons distinguer deux versions de ces approches : *Match-on-Card* (MoC) et *System-on-a-Chip* (SoC).

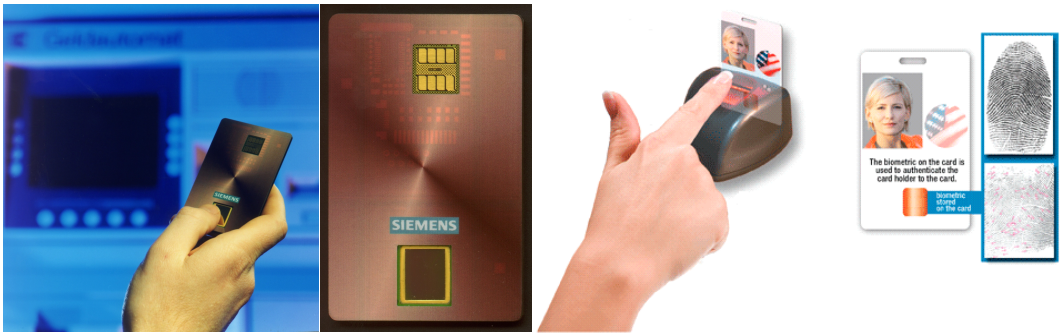
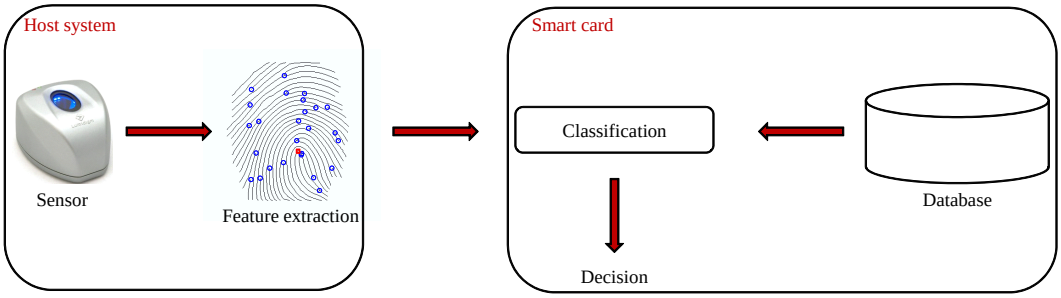
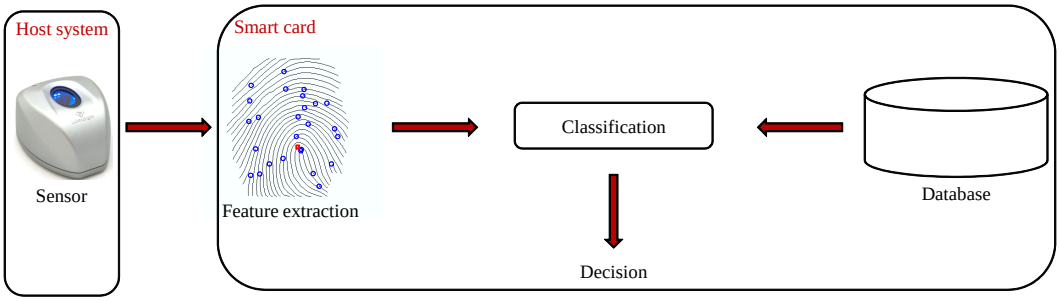


FIGURE 3.2 – Exemples des technologies Match-on-Card et System-on-a-Chip.

Dans la technologie Match-on-Card, la carte à puce contient seulement la base de données et le classifieur (Figure 3.3a). L'utilisateur insère sa carte dans un système hôte qui contient les deux autres modules du système. Le classifieur de la carte effectue une comparaison entre les modèles stockés dans la carte et le modèle envoyés par le système hôte. L'avantage de MoC est que les modèles stockés sont entièrement sécurisés ; car ils circulent seulement à l'intérieur de la carte et seulement la décision de comparaison est envoyée au système hôte. Cependant, même si les modèles d'enrôlement ne peuvent pas être obtenus par un adversaire, un modèle assez similaire peut être obtenu en utilisant l'attaque décrite dans la sous-section 2.5.3 (hill-climbing supportée par un programme de cheval-de-trois ; voir Figure 2.3), sur le module de l'extraction de caractéristiques du système hôte.



(a) Match-on-Card



(b) System-on-a-Chip

FIGURE 3.3 – Architecture et fonctionnement de Match-on-Card et System-on-a-Chip.

Pour résoudre cette vulnérabilité, les concepteurs de la technologie System-on-a-Chip ont proposé de transférer aussi le module de l'extraction de caractéristiques et le classifieur dans la carte à puce (dans certaines versions, aussi le capteur a été transféré) ; pour qu'aucune information biométrique ne quitte la carte sauf la décision finale (Figure 3.3b). L'avantage de SoC est que les seules attaques possibles restantes pour un adversaire sont

les attaques directes contre le capteur (sous-section 2.5.1). Cependant, la conception de System-on-a-Chip est très chère parce qu'elle nécessite des processeurs plus puissants ainsi que plus d'espace mémoire.

En général, l'avantage des approches matérielles des solutions préventives est que les données biométriques ne quittent jamais la carte. Toutefois, cette technologie n'est pas appropriée pour la plupart des applications à grande échelle, car d'une part elle est coûteuse et les utilisateurs doivent porter leurs cartes avec eux tout le temps. D'autre part, car les modèles biométriques peuvent être récupérés à partir d'une carte volée.

3.3.2 Transformation de caractéristiques

L'idée de base des approches de transformation de caractéristiques est de convertir un modèle biométrique non protégé en un modèle protégé en utilisant une fonction de transformation [Ratha *et al.* 2001, Ratha *et al.* 2006]. La fonction de transformation peut prendre plusieurs formes, selon le système et la modalité visée, et elle peut nécessiter aussi l'utilisation de certains paramètres de transformation (par exemple une clef utilisateur). Dans le cas où les modèles biométriques transformés sont volés ou compromis, les paramètres de transformation sont modifiés pour mettre à jour le modèle biométrique protégé. Pour empêcher les imposteurs de suivre les utilisateurs légitimes inscrits dans plusieurs systèmes, et protéger la vie privée par conséquent, il faut appliquer des paramètres de transformation différents ou même des fonctions de transformation différentes pour chaque application.

Généralement, ces approches fonctionnent comme suit (Figure 3.4) : lors de l'enrôlement, une fonction de transformation F est appliquée sur le modèle biométrique original non protégé T en utilisant une clé K ; le modèle transformé F(T,K) est stocké dans la base de données du système. Durant l'authentification / vérification, la même fonction de transformation F est appliquée sur le modèle de test Q. Les modèles protégés F(T,K) et F(Q,K) sont comparés directement dans le domaine de transformation afin de déterminer si l'utilisateur est accepté ou non. La conception de la fonction de transformation F est un problème critique [Jain *et al.* 2008, Rathgeb & Uhl 2011, Campisi 2013], parce que, d'une

part, la fonction F devrait conserver l'individualité / unicité des modèles originaux ; et d'autre part, elle doit être tolérante à la variation intra-sujet des modèles biométriques. En outre, la corrélation de plusieurs modèles transformés ne doit révéler aucune information sur les données biométriques originales (diversité).

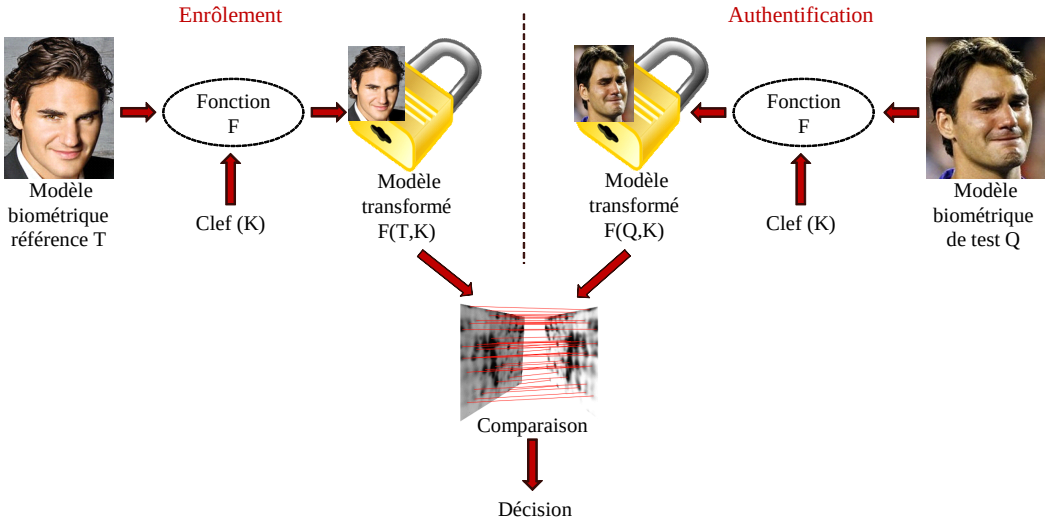


FIGURE 3.4 – Mécanisme général d'authentification d'un système de sécurité biométrique protégé par une approche de transformation de caractéristiques.

Selon la nature et les propriétés de la fonction de transformation F, les approches de transformation de caractéristiques peuvent être divisées en deux classes : la *transformation inversible* (connue sous la dénomination anglaise *Salting* ou aussi *Biohashing*) et la *transformation non inversible* [Jain *et al.* 2008, Rathgeb & Uhl 2011].

Pour la Biohashing, c'est une technique à deux facteurs qui est basée sur l'utilisation de la *projection aléatoire* (*Random projection* en anglais) [Goel *et al.* 2005, Pillai *et al.* 2010]. La projection aléatoire est une technique qui utilise des matrices orthogonales aléatoires pour projeter les modèles biométriques dans d'autres domaines ou espaces où les distances entre les modèles avant et après la transformation sont conservées. La projection aléatoire a été proposée comme une solution autonome pour la protection des modèles biométriques qui essaie de répondre à la propriété de la révocabilité ; et elle est le principe de base de Biohashing. Généralement, pour la Biohashing, des matrices orthogonales aléatoires

sont utilisées pour projeter les modèles biométriques dans un espace où les distances sont préservées. Les étapes de Biohashing sont les suivantes (Figure 3.5) :

- Générer n vecteurs aléatoires en utilisant une clé utilisateur.
- Appliquer l'algorithme de Gram-Schmidt (voir annexe A.2) sur les n vecteurs aléatoires pour calculer une matrice orthogonale Δ.
- Transformer le modèle d'origine z en utilisant la matrice Δ comme suit :

$$y = \Delta z \tag{3.1}$$

  – y est le modèle transformé.

- Quantifier le modèle transformé y comme suit :

$$t_i = \begin{cases} 0 & \text{si } y_i \leq \tau \\ 1 & \text{si } y_i > \tau \end{cases} \quad avec \quad i = 1, \ldots, n \tag{3.2}$$

  – τ est le seuil de comparaison.

  – t est le modèle protégé de taille n.

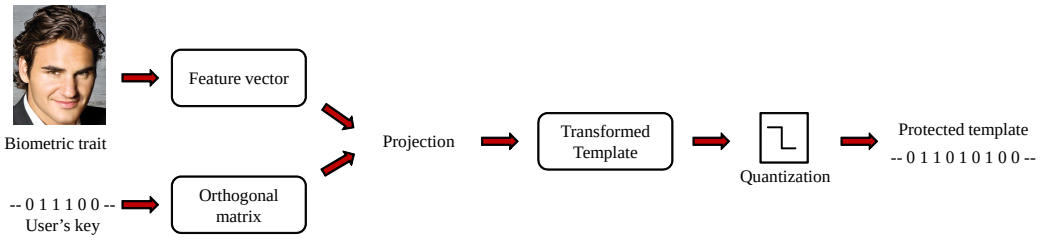


FIGURE 3.5 – Protection des modèles biométriques en utilisant le régime Biohashing.

Il faut noter que plusieurs travaux [Jin *et al.* 2004, Wang & Plataniotis 2007] ont proposé d'appliquer l'étape de quantification (3.2) sur le modèle transformé y pour rendre la projection non inversible. Cependant, il est toujours possible de récupérer le modèle transformé y (ou une approximation de celui-ci) à partir du modèle protégé t en utilisant l'astuce suivante [Nagar *et al.* 2010] :

- Premièrement, nous résolvons le problème des moindres carrés suivant :

$$argmin\|z-r\|_2 \quad subject\ to \quad \begin{cases} y_i \leq \tau & \text{if} \quad t_i = 0 \\ y_i > \tau & \text{if} \quad t_i = 1 \end{cases} \tag{3.3}$$

  - $i = 1,\ldots,n$ et $y_i = \sum_{j=1}^{n} \Delta_{ij} z_i$.
  - r est un vecteur aléatoire de taille n avec $r \times z \leq \tau$.
  - n est la taille du modèle original et du modèle transformé.

- Deuxièmement, afin d'optimiser l'approximation de z, nous résolvons le problème k fois en utilisant k valeurs différentes de r. L'approximation finale $\tilde{z}$ est calculée comme suit :

$$\tilde{z} = \frac{\sum_{i=1}^{k} \frac{z_i}{d_i^2}}{\sum_{i=1}^{k} \frac{1}{d_i^2}} \tag{3.4}$$

  - z_i est le vecteur original estimé en utilisant r_i.
  - $d_i = \frac{1}{d_i'}$ avec d_i' est la distance de Hamming entre z_i et t.

Plusieurs versions de Biohashing sont proposées et adaptées pour la plupart des modalités biométriques [Kong *et al.* 2006, Campisi 2013]. Les méthodes [Chin *et al.* 2006, Pillai *et al.* 2011] sont des exemples de Biohashing dans le contexte des systèmes de la reconnaissance d'iris. Les travaux [Jin *et al.* 2004, Sakata *et al.* 2006] sont des techniques de Biohashing qui sont destinées pour les systèmes de la reconnaissance des empreintes digitales. [Savvides *et al.* 2004, Teoh *et al.* 2006, Kong *et al.* 2006] sont des régimes de Biohashing pour le système de reconnaissance faciale. L'approche *PalmHashing* est un régime de protection spécial qui est destiné aux systèmes de reconnaissance des empreintes palmaires [Connie *et al.* 2005].

Pour la plupart des versions de Biohashing proposées en littérature, la fonction de transformation est inversible. Si un adversaire a un accès au modèle protégé et la clé utilisateur, il peut récupérer le modèle biométrique original (ou une approximation de celui-ci) [Nagar *et al.* 2010]. Par conséquent, la sécurité du régime de Biohashing est basée seulement sur le secret de la clé ou du mot de passe. Alors puisque la transformation est inver-

sible, la clé doit être conservée en toute sécurité par le système et aussi par l'utilisateur pour la présenter lors de l'authentification. Ce besoin d'information supplémentaire sous la forme d'une clé augmente la diversité des modèles biométriques, et les rend plus difficiles à deviner par un adversaire.

Le régime de Biohashing a plusieurs avantages [Jain *et al.* 2008]. Il permet la diversité, car puisque la clé est spécifique à chaque utilisateur, nous pouvons générer plusieurs modèles biométriques (du même utilisateur) en utilisant différentes clés. Ce régime permet aussi la révocabilité, parce que dans le cas où un modèle est compromis, il est facile de le révoquer et le remplacer par un nouveau modèle en utilisant une nouvelle clé utilisateur. Il faut noter que la clé utilisateur ne fournit pas seulement la diversité / révocabilité, mais elle améliore également la performance de reconnaissance [Maltoni *et al.* 2003, Jain *et al.* 2007], ce qui n'est pas surprenant étant donné la nature à *deux facteurs* de ce regime de protection. Concernant les limitations de Biohashing ; si un modèle est compromis, il n'est plus sécurisé. Si l'adversaire a un accès au modèle transformé, il peut récupérer le modèle originale. En général, le choix de la fonction F doit être conçus soigneusement pour que les performances de reconnaissance ne se dégradent pas, parce que la classification se fait dans le domaine de transformation (surtout en présence des variations intra-sujet).

Pour la transformation non inversible (la deuxième catégorie des approches de transformation de caractéristiques). Généralement, un modèle original peut être protégé en utilisant une fonction non inversible [2] qui est dans la plupart des travaux une fonction à sens unique [Rathgeb & Uhl 2011]. En littérature, le principe de la transformation non inversible (bien que le principe de la biométrie révocable) a été proposée pour la première fois par [Ratha *et al.* 2001] (il a été nommé *Cancelable biometrics* dans [Bolle *et al.* 2002]). Dans [Ratha *et al.* 2006, Ratha *et al.* 2007], ces chercheurs ont clarifié et analysé encore bien leur principe proposé. Bien que cette nomination ait été plus tard conçue dans un sens encore plus général pour nommer toutes les approches de protection des modelés biométriques qui sont basées sur une transformation non inversible [Jain *et al.* 2008].

2. L'inversibilité peut être exprimée en termes de la complexité de calcul et le nombre d'essais pour récupérer un modèle original à partir un modèle transformé.

La propriété la plus importante de cette catégorie est que, même si la clé et/ou le modèle transformé sont connus / volés par un adversaire, il est difficile de récupérer le modèle original (en terme de complexité de calcul). Alors les modèles biométriques sont bien protégés. Contrairement aux approches de Biohashing (qui sont la plupart du temps basées sur la projection aléatoire), les fonctions de transformation des approches de transformation non inversible peuvent prendre plusieurs formes (y compris des améliorations de la projection aléatoire qui adressent le problème de l'inversibilité). Les paragraphes suivants présentent un survol sur les formes les plus significatives dans l'état de l'art de cette catégorie [Rathgeb & Uhl 2011, Campisi 2013, Rane *et al.* 2013].

Le régime de protection, appelé *BioPhasor* [Teoh *et al.* 2007], est un exemple de cette catégorie. BioPhasor est une approche basée sur la projection aléatoire qui adresse les exigences de sécurité et d'inversibilité manquantes dans la projection aléatoire traditionnelle et la Biohashing. Les étapes de BioPhasor sont les suivantes :

- Générer m vecteurs aléatoires et les stocker dans une carte à puce infalsifiable.
- Appliquer l'algorithme de Gram-Schmidt (voir annexe A.2) sur les m vecteurs aléatoires pour calculer une matrice orthogonale Δ.
- Transformer le modèle original z (de taille n) en utilisant la formule suivante :

$$y_i = \frac{1}{n}\sum_{i=1}^{n} atan\left(\frac{z_i}{\Delta_{ij}}\right) \tag{3.5}$$

  - $j = 1,\ldots,m \quad m \leq n \quad$ et $\quad \Delta_{ij} \neq 0$.
  - y est le modèle transformé.

- Quantifier le modèle transformé y comme suit :

$$t_i = \begin{cases} 0 & \text{if } 0 < y_i \leq \pi \\ 1 & \text{if } \pi < y_i \leq 0 \end{cases} \quad where \quad i = 1,\ldots,m \tag{3.6}$$

  - t est le modèle protégé de taille m.

L'avantage de BioPhasor par rapport au Biohashing est que la transformation *Arc tan-*

gente améliore l'inversibilité et la sécurité, et elle rend la récupération du modèle original encore plus compliquée. Cependant, il est toujours possible d'avoir une approximation acceptable à partir d'un modèle protégé par BioPhasor (voir annexe A.3).

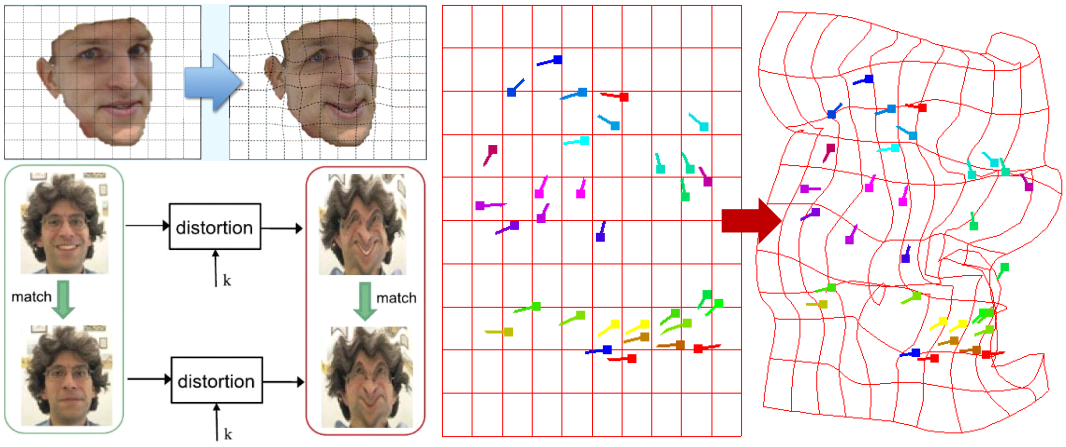


FIGURE 3.6 – Exemples de transformations géométriques appliquées sur le visage et les minuties des empreintes digitales (images prises de [Nagar *et al.* 2010, Campisi 2013, Rane *et al.* 2013]).

L'une des formes de la fonction de transformation les plus significatives dans le contexte des approches de transformation non inversible, est l'utilisation des distorsions ou des transformations géométriques pour protéger les modèles biométriques (Figure 3.6) [Ratha *et al.* 2006, Ratha *et al.* 2007]. Ces transformations varient pour chaque système selon la modalité biométrique utilisée. Le principe de base est d'appliquer une transformation géométrique (contrôlée par certains paramètres) sur les images d'enrôlement (les images transformées sont traitées ensuite par les méthodes standards du système de l'extraction de caractéristiques pour construire les modèles de référence). Au moment de l'authentification / identification, la même transformation doit être appliquée sur les images de test, sinon elles ne correspondront pas aux celles de référence. Ces transformations devraient satisfaire la contrainte que, plusieurs modèles, provenant de différentes distorsions, ne devraient pas se correspondre pour assurer les exigences de la révocabilité / diversité. Par exemple dans [Ratha *et al.* 2007], trois transformations non inversibles (*cartésiennes*, *polaires* et *fonctionnelles*) pour la protection des minuties des empreintes digitales sont proposées.

L'une des limites de ces transformations proposées, est qu'elles peuvent convertir des petites différences de position entre deux minuties dans l'espace original en de grandes différences dans l'espace de transformation (augmentation des variations intra-sujet), ce qui peut conduire à un grand nombre de faux rejets. Ces chercheurs ont recommandé ainsi d'utiliser des transformations lisses pour éviter ce problème et conserver la performance. Cependant, en utilisant une transformation lisse, il serait facile d'inverser le modèle transformé pour récupérer le modèle original. [Boult *et al.* 2007] ont prouvé qu'en pratique, en utilisant ces transformations, seulement 8% de données sont non inversibles. [Quan *et al.* 2008] ont prouvé qu'avec la possession de deux ou plus de modèles transformés du même utilisateur, il est possible de récupérer le modèle original [3].

Bien que la BioPhasor et les approches de distorsion, nous pouvons distinguer autres approches qui appartiennent aux approches de transformation non inversible. Par exemple dans [Maiorana *et al.* 2010], ces chercheurs ont proposé une transformation non-inversible pour protéger les modèles de signatures en ligne. L'idée de base est de considérer le modèle original non protégé comme une série de séquences temporelles distinctes qu'on peut la diviser (selon un vecteur aléatoire) en plusieurs sous-séquences non chevauchantes (le vecteur de division garantit la diversité / révocabilité). Pour générer un modèle transformé, une convolution linéaire de ces sous-séquences peut être appliquée, ce qui rend la récupération du modèle original très difficile du point de vue calculatoire. Le défi majeur de cette approche est la conception des algorithmes de classification qui sont tolérables pour ces convolutions pour éviter la dégradation de la performance.

En littérature, plusieurs approches de transformation non-inversible ont été appliquées et testées sur plusieurs modalités biométriques. Les méthodes [Zuo *et al.* 2008, Hämmerle-Uhl *et al.* 2009, Rathgeb & Uhl 2010c] sont des exemples d'approches de transformation non-inversible destinées aux systèmes de la reconnaissance d'iris. [Sutcu *et al.* 2005, Teoh *et al.* 2007] sont des régimes de protection non-inversible pour les systèmes de reconnaissance faciale. Les travaux [Maiorana *et al.* 2008b, Maiorana *et al.* 2008a, Maiorana *et al.* 2010] sont des schémas de protections des systèmes de signature en ligne. Pour les systèmes de reconnais-

3. Astuce d'attaque prouvée seulement sur les minuties des empreintes digitales.

sance des empreintes digitales, nous pouvons distinguer les travaux significatifs suivants [Lee *et al.* 2007, Chikkerur *et al.* 2008, Ferrara *et al.* 2012].

Généralement, les régimes de transformation non inversible ont plusieurs avantages [Jain *et al.* 2008]. Ils permettent la diversité / révocabilité et ils fournissent une meilleure sécurité par rapport aux approches de Biohashing, car il est difficile de récupérer le modèle original même lorsque la clé utilisateur est volée. L'inconvénient principal de cette approche est la capacité limitée pour fournir l'équilibre entre la discriminative et la non-inversibilité. D'une part, les modèles d'un même utilisateur devraient avoir une grande similitude dans l'espace de transformation, et d'autre part, les modèles de différents utilisateurs devraient être tout à fait dissemblables après la transformation (discriminative). En outre, la fonction transformation doit être également non-inversible. En pratique, il est difficile de concevoir des fonctions de transformation qui fournissent la discriminative et la non-inversibilité, simultanément, en conservant la performance.

3.3.3 Crypto-systèmes biométriques

Dans les crypto-systèmes biométriques [Uludag *et al.* 2004], le principe des crypto-systèmes classiques [Schneier 1995, Ferguson *et al.* 2010] a été combiné avec le principe de la reconnaissance biométrique pour améliorer la sécurité des systèmes d'authentification personnelle basés sur la biométrie. L'objectif principal de ces approches est de minimiser le taux des données biométriques stockées dans les modèles protégés et la base de données du système en général. Le fonctionnement de la plupart des crypto-systèmes biométriques est comme suit : durant l'inscription, on applique un code correcteur d'erreur φ sur le modèle biométrique B et une clé K pour extraire l'ensemble de données H (l'ensemble H est appelé *Helper Data* en anglais). Au moment de l'authentification, on applique un code correcteur d'erreur φ sur les helper data H et le modèle de test Q pour récupérer la clé K (Figure 3.7). Selon la façon dont les helper data sont extraites, les crypto-systèmes biométriques peuvent être divisés en deux catégories [Jain *et al.* 2008, Rathgeb & Uhl 2011] : les crypto-systèmes de type *key-binding* et les crypto-systèmes de type *key-generation*. Lorsque les

helper data sont obtenues en utilisant une clé qui est *indépendante* des caractéristiques biométriques, il s'agit d'un crypto-système de type key-binding. Si les helper data sont dérivées seulement à partir du modèle biométrique et la clé est générée *directement* à partir des caractéristiques biométriques, il s'agit d'un crypto-systèmes de type key-generation.

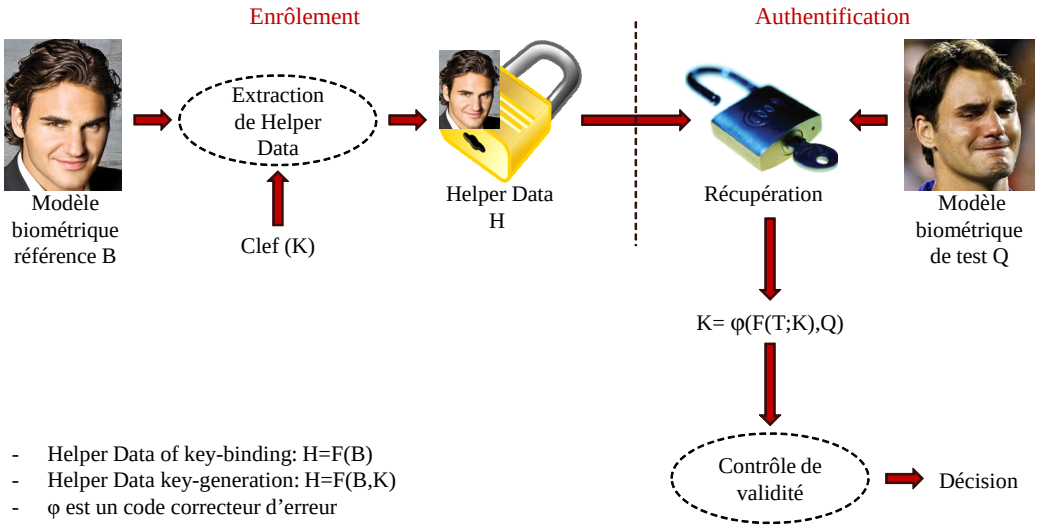


FIGURE 3.7 – Mécanisme général d'authentification des crypto-systèmes biométriques de type key-binding et key generation [Jain *et al.* 2008].

Pour les crypto-systèmes biométriques de type key-binding [Juels & Wattenberg 1999, Hao *et al.* 2006], ils sont tolérants aux variations intra-sujet des modèles biométriques. Cette tolérance peut être interprétée par la capacité du code correcteur d'erreur utilisé. Cependant, ils ne sont pas conçus pour fournir la diversité et la révocabilité. En outre, contrairement aux approches de transformation de caractéristiques, la classification des crypto-systèmes biométriques doit être réalisée en utilisant des codes correcteurs d'erreur, ce qui empêche l'utilisation des classifieurs classiques développés spécifiquement pour comparer les modèles biométriques. Les approches les plus populaires dans cette catégorie sont les systèmes connus sous les nominations : *Fuzzy Commitment* [Juels & Wattenberg 1999] et *Fuzzy Vault* [Juels & Sudan 2002].

Le principe du fonctionnement général de l'approche fuzzy commitment est comme suit [Juels & Wattenberg 1999] : durant l'enrôlement, un *codeword* C est généré aléatoi-

rement pour chaque utilisateur. On calcule le helper data comme la différence du modèle original T et le codeword C (H = T-C) et on stocke H dans la base de données (le hachage *hash*(C) du codeword C est stocké également dans la base de données). Au moment de l'authentification / vérification, on récupère le codeword C en utilisant le modèle de test Q comme suit $C^{'}$= Q-H = Q-(T-C). Ensuite, on applique un code correcteur d'erreur sur $C^{'}$ pour générer $C^{"}$. Pour prendre la décision finale, on compare *hash*(C) avec *hash*($C^{"}$). Le fuzzy commitment a été testé sur plusieurs modalités biométriques. [Hao *et al.* 2006, Rathgeb & Uhl 2010a] sont des exemples de fuzzy commitment pour les systèmes de reconnaissance de l'iris. [Veen *et al.* 2006, Lu *et al.* 2009] sont des exemples de ce schéma de protection dans le contexte des systèmes de reconnaissance faciale. Pour les systèmes de reconnaissance des empreintes digitales, nous pouvons distinguer les travaux significatifs suivants [Teoh & Ong 2008, Nandakumar 2010]. Le fuzzy commitment a été appliqué aussi sur les systèmes de reconnaissance des signatures en ligne [Maiorana & Campisi 2010, Argones Rua *et al.* 2012].

Nous pouvons considérer l'approche fuzzy vault comme une amélioration de fuzzy commitment. Le principe du fonctionnement général de fuzzy vault est comme suit [Juels & Sudan 2002] : durant l'enrôlement, une clé utilisateur K est utilisée pour construire un polynôme P [4]. Ensuite, on calcule la projection polynômiale P(T) du modèle biométrique de référence T. Enfin, on ajoute un peu de bruit à P(T) pour générer le helper data H de fuzzy vault. Au moment de l'authentification / vérification, on applique un code correcteur d'erreur (souvent un code de *Reed-Solomon* [5]) sur le modèle de test Q et le helper data H pour reconstruire le polynôme P et récupérer ainsi la clé K. Le fuzzy vault a été testé sur plusieurs modalités biométriques. [Li *et al.* 2010, Nandakumar *et al.* 2007a, Nguyen *et al.* 2013] sont des exemples pour les systèmes de reconnaissance des empreintes digitales. [Kholmatov & Yanikoglu 2006] est un exemple de ce schéma de protection dans le contexte des systèmes de reconnaissance des signatures en ligne. Pour les systèmes de reconnaissance des empreintes palmaires, il y a le travail [Kumar & Kumar 2008]. Le fuzzy vault a été testé aussi sur les systèmes de

4. le mécanisme de construction de P est comme suit : les coefficients de P sont les chiffres de K et le degré de P est le nombre de ces chiffres moins un. Par exemple, si K=72451 alors P = $7x^4+2x^3+4x^2+5x+1$

5. http ://fr.wikipedia.org/wiki/Code_de_Reed-Solomon

reconnaissance de l'iris dans [Wu *et al.* 2008].

Pour les crypto-systèmes biométriques de type key-generation [Monrose *et al.* 2001, Chang *et al.* 2004, Blanton & Aliasgari 2013], ils souffrent généralement d'une discriminative faible, qui peut être évaluée en termes de stabilité de clé [6] et d'entropie de clé [7] [Jain *et al.* 2008]. Si un régime génère la même clé quel que soit le modèle d'entrée, alors il y a une grande stabilité de clé mais une entropie nulle, ainsi il aura un taux élevé de fausses acceptations. Si le système génère des clés différentes pour différents modèles d'un même utilisateur, alors le système a une entropie élevée mais une stabilité nulle, et cela conduit à un taux élevé de faux rejets. Alors le grand défi dans la conception de ces schémas de protection est d'atteindre simultanément une stabilité de clé et une grande entropie. Les approches les plus populaires dans cette catégorie sont les systèmes connus sous les nominations : *Secure Sketch* [Bringer *et al.* 2008] et *Fuzzy Extractor* [Dodis *et al.* 2008].

Le but de régimes Secure Sketch est de gérer les variations intra-sujet des modèles biométriques par la minimisation des informations biométriques dans les *sketchs* (les modèles protégés sont appelés *sketchs* dans un crypto-système Secure Sketch). Cependant, ces approches n'arrivent pas à équilibrer efficacement la stabilité / entropie de la clé. Le fuzzy extractor peut être considéré comme une amélioration de Secure Sketch qui adresse la gestion des variations intra-sujet et la stabilité / entropie de la clé simultanément. Ces deux versions des crypto-systèmes biométriques de type key-generation ont été testées sur plusieurs modalités biométriques. Les méthodes [Arakala *et al.* 2007, Li *et al.* 2008, Yang *et al.* 2012] sont des exemples des crypto-systèmes biométriques de type key-generation pour les systèmes de la reconnaissance des empreintes digitales. [Zhou 2007, Sutcu *et al.* 2007] sont des crypto-systèmes key-generation destinés pour les systèmes de reconnaissance faciale. Les travaux [Feng & Wah 2002, Vielhauer *et al.* 2002] sont des schémas de protections des systèmes de signature en ligne. Ce schéma de protection a été testé aussi dans le contexte des systèmes de reconnaissance de l'iris dans [Rathgeb & Uhl 2010b].

Selon la norme ISO/IEC 24745 [ISO/IEC 2011], il n'est pas toujours clair comment

6. Taux de répétibilité d'une clé générée à partir les données biométriques
7. Nombre de clés possibles (différentes) qui peuvent être générées

les crypto-systèmes biométriques affecteront la précision / performance globale des systèmes protégés en termes de taux de faux rejets et de fausses acceptations. En outre, peu de travaux ont été faits pour tester les attaques possibles contre les crypto-systèmes biométriques, alors leur sécurité est largement inconnue. Dernièrement, des analyses de sécurité, comme [Blanton & Aliasgari 2013], ont prouvé que ces schémas de protection sont toujours vulnérables à un certain nombre d'attaques et qu'ils ne peuvent pas être réutilisés, en toute sécurité, s'ils ont été déjà compromis.

3.3.4 Approches hybrides

Quand une méthode de protection des modèles biométriques se base sur plus d'un des quatre approches de base (biohashing, transformation non-inversible, crypto-système key-binding et crypto-système key-generation) présentées dans les sous-sections 3.2 et 3.3 ; on l'appelle une approche *hybride* de protection des modèles biométriques. Ces approches hybrides essaient de combiner les avantages de plusieurs régimes de protection de base sans souffrir de leurs inconvénients respectifs.

Par exemple dans [Feng *et al.* 2010], une approche hybride pour les systèmes de reconnaissance faciale est proposée. Le processus de protection des modèles biométriques se déroule selon trois étapes. Premièrement, une projection aléatoire (standard sans binarisation) est appliquée sur le modèle original non protégé pour générer un modèle transformé. Deuxièmement, une étape de binarisation (appelée *Discriminability Preserving Transform* ; qui est la contribution majeure de ce travail) est appliquée sur le modèle transformé pour conserver la discriminative et générer des modèles binaires compatibles avec le fonctionnement des crypto-systèmes biométriques de type key-binding. Enfin, le crypto-système fuzzy commitment est appliqué aux modèles binaires pour générer les modèles protégés finaux de cette approche hybride. Ce régime est relativement capable de fournir toutes les exigences nécessaires dans un schéma de protection (révocabilité, diversité, sécurité et performance). Cependant, comme dans les crypto-systèmes biométriques, la conception de cette approche exige toujours l'utilisation d'un code correcteur d'erreur dans la phase de

classification et empêche l'utilisation des classifieurs biométriques classiques. Les travaux [Voderhobli *et al.* 2006, Nandakumar *et al.* 2007b, Boult *et al.* 2007, Song *et al.* 2008] sont d'autres exemples qui peuvent être considérés comme des approches hybrides pour la protection des modèles biométriques.

3.4 Résumé du chapitre et conclusions

Dans ce chapitre, nous avons présenté l'état de l'art des approches de protection des systèmes biométriques. Nous avons commencé par la description des solutions palliatives qui visent la plupart du temps les attaques directes contre l'interface utilisateur des systèmes biométriques. Ensuite, nous avons mis l'accent sur les solutions préventives, qui visent généralement la protection des modèles biométriques, en accordant une attention particulière aux approches de transformation non-inversible.

Généralement, il n'y a pas une meilleure approche pour la protection des modèles biométriques ; et les régimes de protection disponibles ne sont pas encore suffisamment matures pour le déploiement à grande échelle, et ne répondent pas, simultanément et efficacement, aux exigences de révocabilité, diversité, sécurité et haute performance. A cause de ces limitations, il est très important d'utiliser des méthodes d'évaluation de performance / sécurité pertinentes et rigoureuses pour quantifier correctement et efficacement les solutions de protection disponibles ; pour être capable ainsi de clarifier mieux leurs avantages / inconvénients et les évoluer correctement. C'est le but du chapitre suivant.

"If you cannot measure it, you cannot improve it"

WILLIAM THOMSON

CHAPITRE 4

Évaluation de performance et de sécurité des schémas de protection

Sommaire

4.1 Introduction 57
4.2 Evaluation de performances 58
4.2.1 Convivialité des systèmes biométriques 59
4.2.2 Protocole FVC 62
4.3 Évaluation de sécurité 64
4.3.1 Vulnérabilité aux attaques d'intrusion 65
4.3.2 Vulnérabilité à la liaison de bases de données 66
4.4 Résumé du chapitre et conclusions 67

4.1 Introduction

Dans ce chapitre, nous allons présenter les critères de performance et de sécurité qui vont être utilisés dans le chapitre 5 pour analyser les deux approches proposées dans cette thèse (*Spiral Cube* et F*ingerprint Shell*). La performance sera analysée en terme des taux d'erreur [Adler & Schuckers 2007]. La sécurité sera analysée en terme de robustesse contre les attaques qui visent les modèles biométriques. L'analyse de la sécurité des systèmes existants est principalement basée sur la complexité des attaques à force brute qui suppose que les données biométriques sont uniformes. Cependant, en pratique, un adversaire peut exploiter la nature non uniforme des données biométriques pour lancer une attaque qui peut exiger beaucoup moins de tentatives pour atteindre la sécurité du système. Alors une analyse de sécurité rigoureuse, comme celle de [Nagar *et al.* 2010], est très nécessaire pour analyser correctement la sécurité des approches de protection des modèles biométriques.

Dans ce chapitre, dans un premier temps, les critères généraux pour évaluer la convivialité des systèmes biométriques sont abordés (sous-section 4.2.1). Ensuite, nous allons détailler le protocole FVC [Maio *et al.* 2002, Maltoni *et al.* 2003, Cappelli *et al.* 2006] (*Fingerprint Verification Competition* protocol) dans la sous-section 4.2.2, qui sera très utile pour évaluer la convivialité de notre approche Fingerprint Shell et pour la comparer correctement et d'une manière équitable avec les approches les plus significatives dans l'état de l'art. Dans la section 4.3, nous allons détailler plusieurs équations analytiques, basées sur [Nagar *et al.* 2010], pour mesurer la résistance des approches de transformation de caractéristiques face à divers types d'attaques qui menacent les modèles biométriques.

4.2 Evaluation de performances

Dans cette section, nous allons présenter les valeurs statistiques, FRR et FAR (abréviations de *False Reject Rate* et *False Accept Rate* respectivement), utilisées en littérature pour évaluer la performance d'un système biométrique. Bien que ces valeurs statistiques sont intuitivement faciles à comprendre, il est difficile d'établir une définition claire et universelle pour ces valeurs ; parce que plusieurs facteurs, qui diffèrent d'un système à un autre, doivent être pris en considération. Mais tout d'abord, il faut clarifier les modes de fonctionnement d'un système biométrique (authentification, identification et vérification), qui sont utiles pour mieux comprendre les notions de FRR / FAR et les critères de l'analyse de sécurité présentés dans la section 4.3.

Un système biométrique fonctionne habituellement selon deux modes principaux : l'enrôlement et l'authentification. Dans l'étape de l'enrôlement, le système capture les traits biométriques des utilisateurs et applique une extraction de caractéristiques pour construire un modèle biométrique de référence qui sera stocké dans la base de données du système. Pour l'authentification, nous pouvons la définir comme le processus de détermination de l'identité d'une personne et la confirmation de son authenticité. L'étape de l'authentification est mise en œuvre différemment selon l'objectif de la conception du système : soit pour la *vérification* ou l'*identification* des utilisateurs.

Dans un système de vérification [1], l'utilisateur fournit son trait biométrique de test et aussi son identité (par exemple dans les systèmes de vérification commerciaux, l'utilisateur est invité à faire entrer son numéro d'inscription avant de présenter ses trais biométriques). Le modèle de test extrait est comparé *seulement* avec le modèle de référence stocké dans la base de données qui correspond à cette identité pour prendre la décision finale.

Dans un système d'identification [2], contrairement au système de vérification, l'utilisateur fournit seulement son trait biométrique. Le modèle de test extrait est comparé avec tous les modèles de référence stockés dans la base de données du système. Si l'un des modèles de référence correspond au modèle de test, le système déclare cette identité, sinon le système déclare une non-concordance.

Cette thèse porte essentiellement sur les systèmes de vérification car la sécurité des modèles biométriques est plus critique et préoccupante dans le cas des applications commerciales et gouvernementales qui sont la plupart du temps basées sur la vérification comme un mode d'authentification. Cependant, il faut noter que nos deux approches proposées dans cette thèse peuvent être utilisées aussi dans le contexte d'un système d'identification.

4.2.1 Convivialité des systèmes biométriques

FAR (False Accept Rate) est la probabilité qu'une personne non autorisée sera acceptée par le système. FAR est une mesure de sécurité pertinente, car une fausse acceptation peut souvent conduire à des dégâts critiques. La probabilité de succès contre une personne légitime θ est :

$$FAR(\theta) = \frac{number\ of\ successful\ fraud\ attacks}{total\ number\ of\ fraud\ attacks} \tag{4.1}$$

- Dans une attaque de fraude, le système est attaqué par un modèle d'une personne non autorisée qui essaie de contourner le système.
- L'attaque de fraude est réussie si la distance entre le modèle de la personne θ et le modèle de l'adversaire est *inférieure ou égale* à un seuil ε.

1. University of Bologna, Biometric System Laboratory, FVC-onGoing : on-line evaluation of fingerprint recognition algorithms. https ://biolab.csr.unibo.it/fvcongoing/UI/Form/Home.aspx

2. FBI-IAFIS : Integrated Automated Fingerprint Identification System of the American Federal Bureau of Investigation. http ://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis

Le FAR final pour Φ utilisateurs est la moyenne de tous les FAR(θ) (pour une seule valeur de ε) :

$$FAR = \frac{1}{\Phi} \sum_{\theta=1}^{\Phi} FAR(\theta) \tag{4.2}$$

En raison de la nature statistique du FAR, un grand nombre d'attaques fraudes doivent être réalisées pour obtenir des résultats fiables. En outre, les attaques fraudes doivent être indépendantes et effectuées avec des identités différentes. Il faut noter que FAR n'est pas suffisante pour valoriser la sécurité d'un système (seulement pour mesurer relativement la résistance contre les *attaques à force brute*), car il y a beaucoup d'autres possibilités pour lancer des attaques prometteuses comme nous l'avons mentionné précédemment.

FRR (False Reject Rate) est la probabilité qu'une personne légitime sera rejetée par le système. FRR est un critère de confort, car un faux rejet réduit la crédibilité des systèmes biométriques. Cette valeur ne dépend pas seulement de la conception du système mais des utilisateurs également. La probabilité de défaillance d'une personne légitime θ est :

$$FRR(\theta) = \frac{number\ of\ rejected\ verifications}{total\ number\ of\ verifications} \tag{4.3}$$

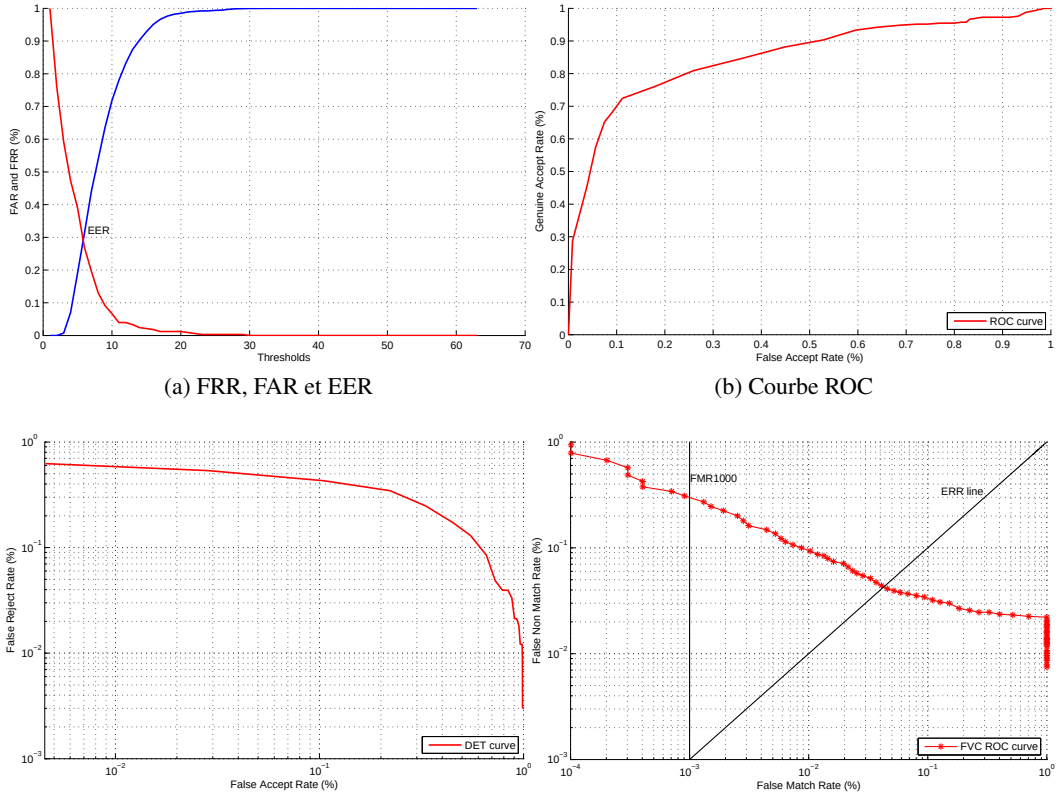
– Une vérification est rejetée si la distance entre le modèle de la personne θ et le modèle de référence est *strictement supérieure* à un seuil ε.

Le FRR final de Φ utilisateurs est la moyenne de tous les FRR (θ) (pour une seule valeur de ε) :

$$FRR = \frac{1}{\Phi} \sum_{\theta=1}^{\Phi} FRR(\theta) \tag{4.4}$$

En pratique, les courbes FAR / FRR sont parfaitement adaptées pour définir le seuil optimal pour faire fonctionner un système. Alors on trace le FRR contre le FAR pour constuire la courbe ROC (Receiver Operating Characteristic) [Maio *et al.* 2002]. Cette courbe est utilisée pour mesurer la convivialité d'un système biométrique. Nous pouvons tracer la courbe ROC dans deux scénarios : le ROC_o original (avant la protection) et le ROC_t de transformation pour indiquer la dégradation des performances due aux régimes de protection.

Comme les courbes ROC des bons systèmes se trouvent très près des axes de coordonnées, il est raisonnable de tracer un ou deux axes en utilisant une échelle logarithmique pour une meilleure visualisation. Il faut noter que dans quelques travaux, le terme DET (Detection Error Tradeoff) est utilisé au lieu de ROC. Dans ce cas, le terme ROC est réservé pour la courbe de 1-FRR contre FAR (1-FRR est appelé *Genuine Accept Rate* (GAR)). Nous utilisons dans cette thèse la deuxième notation.



(a) FRR, FAR et EER

(b) Courbe ROC

(c) Courbe DET

(d) Courbe ROC selon le protocole FVC

FIGURE 4.1 – Exemples des courbes FAR, FRR, DET, ROC et le point EER.

La valeur EER (Equal Error Rate) est calculée comme le point où FRR(ε)=FAR(ε). Il convient de noter que les valeurs de EER dépendent également des définitions de FAR / FRR. Alors une comparaison de deux valeurs EER qui appartiennent à deux différents systèmes est raisonnable seulement si ses définitions se coïncident. La Figure 4.1 présente des exemples de ces courbes / valeurs. La Figure 4.1(a) est un exemple de courbes FAR et FRR et son intersection EER. La Figure 4.1(b) est un exemple de la courbe ROC selon la

deuxième notation et la Figure 4.1(c) est un exemple de la courbe DET.

Dans notre analyse, nous allons utiliser un autre critère d'évaluation [El-Abed 2006], pour mesurer la convivialité et surtout l'*efficacité* d'un schéma de protection :

$$Efficiency = 1 - \frac{AUC\,(ROC_t)}{AUC\,(ROC_o)} \tag{4.5}$$

– AUC (Area Under Curve) est l'aire sous la courbe ROC.

La valeur de cette mesure devrait être positive et proche de 1 que possible. Plus *Efficiency* est proche de 1, meilleure est la robustesse du système contre l'attaque de fraude.

4.2.2 Protocole FVC

FVC est l'abréviation de *Fingerprint Verification Competition*. Il s'agit d'une compétition internationale qui a été organisée (par des laboratoires académiques) pour évaluer des algorithmes de vérification d'empreintes digitales qui appartiennent à des académiques et des gens d'industrie également. Plusieurs bases de données (FVC2000, FVC2002, FVC2004 et FVC2006), qui sont acquises avec divers types de capteurs, ont été fournies aux participants pour leur permettre de tester leurs algorithmes en respectant un protocole de test prédéfini. Le but de cette sous-section est de détailler ce protocole FVC, qui sera utilisé pour tester notre algorithme *Fingerprint Shell* dans le chapitre suivant.

Dans ce protocole, pour chaque base de données FVC (chaque personne est représentée par 8 impressions), la première impression de chaque doigt est comparée avec la première impression des autres doigts pour obtenir la distribution de scores des imposteurs (*impostor score distribution* en anglais). Pour obtenir la distribution de scores des légitimes (*genuine score distribution* en anglais), chaque empreinte est comparée aux impressions restantes du même doigt (même identité). Il convient de noter que dans le protocole FVC, les scores calculés doivent être dans l'intervalle [0, 1], et les comparaisons symétriques ne sont pas lancées pour éviter la répétition des scores (par exemple, si un modèle biométrique T_1 est déjà comparé avec un modèle T_2, alors le score de T_2 contre T_1 ne sera pas calculé).

La distribution des scores légitime / imposteur peut être illustrée graphiquement pour

montrer comment un algorithme peut séparer ou distinguer entre les imposteurs et les utilisateurs légitimes (Figure 4.2).

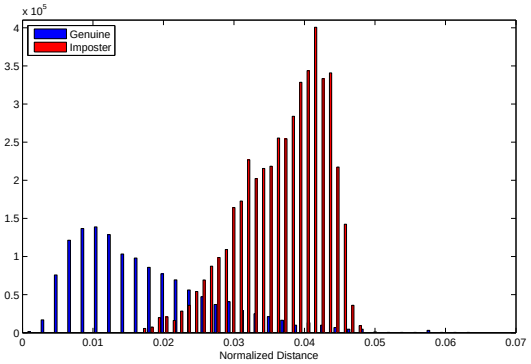


FIGURE 4.2 – Exemple d'un histogramme de distribution des scores légitime / imposteur.

Dans notre évaluation, nous utiliserons aussi deux autres facteurs pour mesurer la séparabilité des scores : premièrement, le test de Kolmogorov-Smirnov (K-S test) [Holland & Komogortsev 2013]. Plus ce test est proche de 1, meilleure est la séparation des scores, ce qui signifie que la diversité est grande. Deuxièmement, le critère de séparabilité proposé par [Lee *et al.* 2007] :

$$Separability = \frac{|\,\mu_G - \mu_i\,|}{\sqrt{\left(\sigma_G^2 + \sigma_i^2\right)/2}} \tag{4.6}$$

– μ_G et μ_i sont la moyenne de distributions des légitimes et imposteurs respectivement.

– σ_G^2 et σ_i^2 sont la variance de distributions des légitimes et imposteurs respectivement.

Selon le protocole FVC, les *genuine matching scores* (gms) et les *impostor matching scores* (ims) sont utilisées pour calculer le *False Match Rate* (FMR) et le *False Non Match Rate* [3] (FNMR). Pour un seuil t allant de 0 à 1 [Maio *et al.* 2002] :

$$FMR(t) = \frac{cardinality\{ims | ims \geq t\}}{number\ of\ impostor\ recognition\ attempts} \tag{4.7}$$

$$FNMR(t) = \frac{cardinality\{gms | gms < t\} + REJ}{number\ of\ genuine\ recognition\ attempts} \tag{4.8}$$

– *REJ* est le nombre de rejets. Si une image ne peut pas être inscrite avec succès dans le

3. FNMR a été défini d'une manière différente dans le protocole FVC par rapport au FNMR de référence.

système, le score de comparaison sera 0 pour toutes les tentatives de reconnaissance possibles en utilisant un des modèles rejetés.

On trace FNMR en fonction de FMR pour obtenir la courbe ROC du protocole FVC en utilisant une échelle logarithmique dans les deux axes (Figure 4.1(d))[4].

Nous allons utiliser autres indicateurs supplémentaires de performance dans notre évaluation [Cappelli *et al.* 2006] : premièrement, FMR_{1000} qui est égale à la valeur de FNMR quand FMR=0.001%. Deuxièmement, Zero_{FMR} qui est égale à la *plus petite* valeur de FNMR quand FMR=0%. Ces valeurs sont utilisées pour évaluer la précision performance des systèmes de vérification qui opèrent loin du point *Equal Error Rate* (EER) (en pratique, il y a des systèmes qui visent de haute sécurité, alors ils utilisent un seuil qui réduit FMR même si cela donne un FNMR élevé. C'est le cas de la plupart des systèmes commerciaux).

4.3 Évaluation de sécurité

Comme nous l'avons détaillé dans la section 2.5, un adversaire peut voler et exploiter les modèles biométriques stockés dans la base de données pour lancer plusieurs attaques, qui peuvent être classées généralement en deux catégories : les attaques d'*intrusion* et les attaques de *liaison de bases de données* (*linkage* ou *cross-matching* en anglais).

Les attaques d'intrusion comprennent les attaques par rejeu (voir section 2.5.2), l'attaque hill-climbing (voir sections 2.5.3 et 2.5.2) et la régénération des traits biométriques et la création d'une parodie physique (voir section 2.5.4 et 2.5.1). Dans les attaques de liaison de bases de données, un adversaire peut exploiter deux modèles qui appartiennent à la même personne, et qui sont volés à partir de deux différentes bases de données, pour suivre les activités de cette personne et plagier son identité. En outre, si ces deux modèles contiennent des informations biométriques différentes, l'adversaire peut lier ces informations pour récupérer un modèle encore plus proche au modèle original.

Dans les sous-sections 4.3.1 et 4.3.2, nous allons détailler plusieurs équations analy-

4. Les notions de FMR et FNMR coïncident souvent en littérature avec les notions de FAR et FRR respectivement. Cependant, la notation FAR / FRR est différente et même trompeuse dans certaines applications. Consultez la page 407 de [Maio *et al.* 2002] pour plus de détails.

tiques, basées sur [Nagar *et al.* 2010], pour mesurer la résistance des approches de transformation de caractéristiques aux attaques d'intrusion et de liaison de bases de données.

4.3.1 Vulnérabilité aux attaques d'intrusion

Pour mesurer la vulnérabilité des approches de transformation de caractéristiques à des attaques d'intrusion, nous considérons le scénario où un modèle protégé est volé à partir de la base de données et que les paramètres de transformation sont connus par l'attaquant. Dans ce scénario, l'adversaire va essayer de récupérer le modèle original et rejouer le modèle récupéré (dans le *même* système) en utilisant les paramètres de transformation. Ce critère a été nommé IRIS (*Intrusion Rate due to Inversion for the Same* biometric system) :

$$IRIS(\varepsilon) = P\left[D\left(f\left(f^{-1}\left(T_i, k_i\right), k_i\right), T_i\right) < \varepsilon\right] \tag{4.9}$$

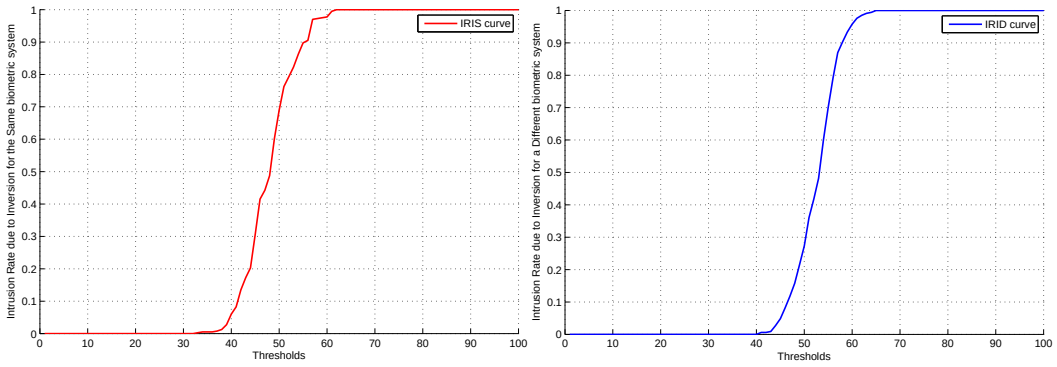
- D est la fonction de distance.
- f est la fonction de transformation.
- f^{-1} est la fonction de transformation inverse.
- $T_i = f\left(t_i, k_i\right)$ est le modèle transformé volé.
- t_i est le modèle original de l'identité i.
- k_i sont les paramètres de transformation de l'identité i.

Considérant le scénario précédent, mais cette fois nous allons supposer que l'adversaire lance une attaque contre un *autre* système biométrique qui contient la même identité volée ou compromise, en supposant que l'attaquant connaît aussi les paramètres de transformation du deuxième système. Ce critère a été nommé IRID (*Intrusion Rate due to Inversion for a Different* biometric system) :

$$IRID(\varepsilon) = P\left[D\left(f\left(f^{-1}\left(T_i, k_i\right), k_i^{'}\right), T_i^{'}\right) < \varepsilon\right] \tag{4.10}$$

- $T_i^{'} = f\left(t_i^{'}, k_i^{'}\right)$ est le modèle transformé de l'identité i dans le deuxième système.
- $t_i^{'}$ est le modèle original de l'identité i dans le deuxième système.

– k_i' sont les paramètres de transformation de l'identité i dans le deuxième système.


IRIS curve
Intrusion Rate due to Inversion for the Same biometric system
Thresholds
IRID curve
Intrusion Rate due to Inversion for a Different biometric system
Thresholds

(a) IRIS curve (b) IRID curve

FIGURE 4.3 – Exemples des courbes IRIS et IRID.

IRIS et IRID dépendent du seuil ε. Il est facile d'inverser un modèle biométrique, protégé par une approche de transformation de caractéristiques, si IRIS et IRID sont à proximité de ou égal à 1 (Figure 4.3).

4.3.2 Vulnérabilité à la liaison de bases de données

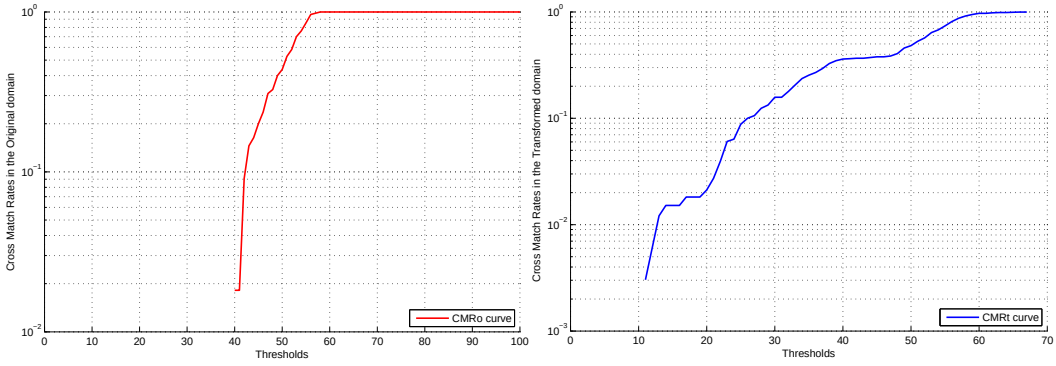
La vulnérabilité des approches de transformation de caractéristiques aux attaques de liaison de bases de données peut être mesurée en considérant le scénario où l'adversaire vole deux modèles biométriques d'une même identité à partir de deux systèmes différents qui utilisent le même schéma de protection ; en supposant que l'attaquant connaît les paramètres de transformation de ces deux systèmes. L'adversaire peut lancer son attaque soit dans le domaine original ou dans le domaine de la transformation. Ce critère a été nommé CMR (*Cross-Matching Rate*). Nous pouvons calculer CMR dans ces deux domaines comme suit :

$$CMR_o(\varepsilon) = P\left[D\left(f^{-1}(T_i,k_i), f^{-1}(T_i',k_i')\right) < \varepsilon\right] \tag{4.11}$$

– CMR_o est le taux de liaison de bases de données dans le domaine original.

$$CMR_t(\varepsilon) = P\left[D\left(f(t_i,k_i), f(t_i',k_i')\right) < \varepsilon\right] \tag{4.12}$$

– CMR_t est le taux de liaison de bases de données dans le domaine de transformation.



(a) CMR_o curve (b) CMR_t curve

FIGURE 4.4 – Exemples des courbes CMR_o et CMR_t.

Bien que le test de Kolmogorov-Smirnov (K-S test) [Holland & Komogortsev 2013] (qui est pour mesurer la diversité), une étude des attaques de de liaison de bases de données est très utile aussi pour mesurer la diversité des approches de transformation de caractéristiques. Figure 4.4 est un exemple de l'interprétation graphique de CMR_o et CMR_t.

4.4 Résumé du chapitre et conclusions

Dans ce chapitre, nous avons présenté les critères d'évaluation de performance et de sécurité qu'on va utiliser dans le chapitre suivant pour tester et comparer notre deux approches proposées avec les approches existantes. Nous avons commencé par la description des critères généraux pour évaluer la convivialité des systèmes biométriques. Ensuite, nous avons détaillé le protocole d'évaluation FVC. Enfin, nous avons présenté les équations analytiques pour mesurer la vulnérabilité des approches de transformation de caractéristiques aux attaques d'intrusion et de liaison de bases de données.

CHAPITRE 5

Nouvelles approches de protection des modèles biométriques

Sommaire

5.1 Introduction 69
5.2 Spiral Cube pour la protection des modèles biométriques 70
5.2.1 Introduction 70
5.2.2 Suite logistique 71
5.2.3 Spiral Cube 74
5.2.4 Expérimentations et discussion 77
5.2.4.1 Bases de données et procédures d'experimentation 77
5.2.4.2 Évaluation en utilisant la base de données YALE 80
5.2.4.3 Évaluation en utilisant la base de données PolyU FKP . . 85
5.2.4.4 Évaluation en utilisant la base de données CASIA 89
5.2.4.5 Évaluation en utilisant la base de données UMIST 92
5.2.4.6 Performance avec des modèles de grandes tailles 95
5.3 Fingerprint Shell pour la protection des minuties 96
5.3.1 Introduction 96
5.3.2 Reconnaissance des empreintes digitales 98
5.3.3 Travaux connexes 100
5.3.4 Fingerprint Shell 102
5.3.5 Expérimentations et discussion 105
5.4 Résumé du chapitre et conclusions 110

5.1 Introduction

Dans ce chapitre, nous allons présenter deux nouvelles approches de la protection des modèles biométriques, qui ont été proposées lors de l'élaboration de cette thèse. Les méthodes proposées sont :

1. *Spiral Cube* [Moujahdi *et al.* 2012] : Approche de protection des modèles biométriques pour sécuriser les systèmes biométriques qui utilisent des modèles biométriques sous forme de vecteurs. Cette technique est basée sur la projection aléatoire et le comportement chaotique de la suite logistique.

2. *Fingerprint Shell* [Moujahdi *et al.* 2014a] : Approche de protection des modèles biométriques qui visent les systèmes de reconnaissance des empreintes digitales qui utilisent des modèles biométriques représentés sous forme de minuties. Dans cette technique, une nouvelle représentation est utilisée au lieu des modèles traditionnels basés sur les minuties.

Dans ce chapitre, une propre section est consacrée à chacune des nouvelles méthodes. L'approche Spiral Cube sera présentée dans la section 5.2 et l'approche de Fingerprint Shell sera présentée dans la section 5.3. Ces deux sections partagent une structure commune : Une brève introduction du problème visé, ensuite une description de l'approche, et enfin une présentation et discussion des résultats expérimentaux. Le résumé du chapitre et les conclusions seront l'objet de la section 5.4.

5.2 Spiral Cube pour la protection des modèles biométriques

5.2.1 Introduction

L'utilisation croissante de la biométrie pour la conception des systèmes de sécurité a déclenché un regain d'intérêt pour la recherche et l'exploration de nouvelles méthodes pour attaquer les systèmes biométriques. Ces recherches ont prouvé que la biométrie a donné lieu à de nouveaux problèmes et défis liés à la sécurité et la protection des données personnelles (section 2.5) ; problèmes qui sont encore plus compliqués que ceux des systèmes traditionnels. Les attaques contre les modèles biométriques, stockés dans la base de données du système, présentent une préoccupation majeure pour la sécurité et la vie privée des systèmes d'authentification biométriques (sous-section 2.5.4).

Dans cette section, nous présentons une nouvelle approche pour la protection des mo-

dèles biométriques. Notre objectif est de construire une approche de transformation non inversible (sous-section 3.3.2), basée sur la projection aléatoire, qui répond aux exigences de la révocabilité, la diversité, la sécurité et la performance (section 2.7). Dans ce contexte, on utilise le comportement chaotique de la suite logistique pour construire les vecteurs de projection en recourant à une technique qui rend la construction de la matrice de projection dépendante du modèle biométrique et son identité. L'approche proposée a été évaluée et comparée avec Biohashing et BioPhasor (section 3.3.2) en utilisant une analyse de sécurité rigoureuse (section 4.3). Nos résultats expérimentaux, qui sont obtenus en utilisant plusieurs bases de données / modalités (visage, finger-knuckle et iris), montrent que la technique proposée a la capacité de préserver et d'accroître la performance des systèmes protégés. En outre, il est démontré que la sécurité de cette approche est suffisamment robuste contre les attaques possibles et elle fournit un équilibre acceptable entre la discrimination, la diversité et la non-inversibilité.

Le reste de la section est organisé comme suit : dans la sous-section 5.2.2, le phénomène de chaos, la suite logistique et la procédure de construction de la matrice 'Spiral Cube' sont abordés. La sous-section 5.2.3 détaille le fonctionnement de l'approche proposée. Nos résultats expérimentaux, les comparaisons et la discussion sont présentés dans la sous-section 5.2.4.

5.2.2 Suite logistique

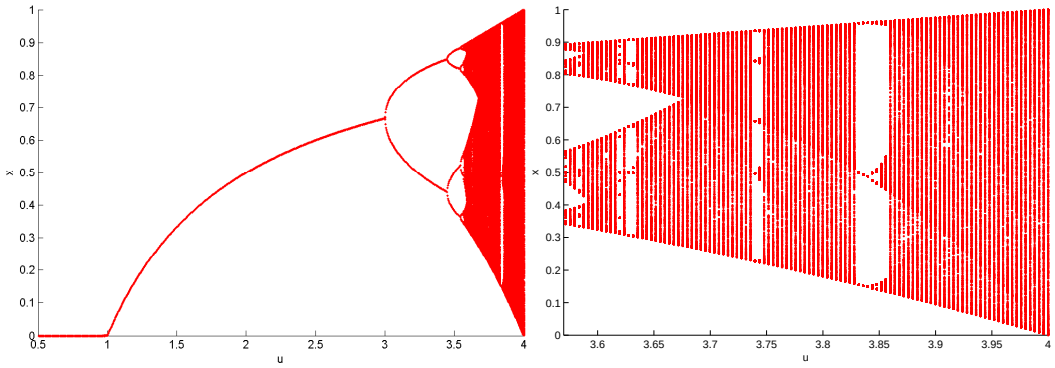
La suite logistique [1] (*logistic map* en anglais) est une suite simple qui est définie par récurrence. Cette suite est caractérisée par une récurrence qui n'est pas linéaire. Mathématiquement, la suite logistique est définie comme suit :

$$x_{n+1} = \mu x_n (1 - x_n) \tag{5.1}$$

Selon la valeur de μ, nous pouvons observer un comportement chaotique dans l'intervalle [3.5699456, 4] (Figure 5.1). On appelle cette propriété : la *sensibilité aux conditions*

1. http ://en.wikipedia.org/wiki/Logistic_map

initiales (*SIC* ou S*ensitivity to Initial Conditions* en anglais). D'une manière simple, SIC veut dire que si nous avons un petit changement / perturbation arbitraire dans les conditions actuelles, alors on va avoir un comportement futur significativement très différent. En exploitant cette propriété de la suite logistique, elle a été utilisée dans plusieurs applications, y compris la sécurité des informations. Par exemple, les séquences aléatoires de la zone chaotique peuvent être utilisées pour sécuriser cryptographiquement les canaux de transmission dans les systèmes biométriques [Bhatnagar & Wu 2012] et dans les systèmes de télécommunications également [Zhang *et al.* 2013].



(a) Intervalle *[0.5, 4]* (b) Intervalle chaotique *[3.5699456, 4]*

FIGURE 5.1 – Implémentation de la suite logistique dans l'environnement Matlab.

Comme nous avons vu dans la description de la projection aléatoire, Biohashing et BioPhasor dans la section 3.3.2 et l'annexe A.1, l'algorithme d'orthogonalisation de Gram-Schmidt génère un ensemble de vecteurs orthogonaux si et seulement si les vecteurs d'entrée sont linéairement indépendants. Par conséquent, la génération des vecteurs aléatoires en utilisant une clé utilisateur (dans Biohashing et BioPhasor) sera relativement limitée par cette exigence. Cela nous a motivé à utiliser le comportement chaotique de la suite logistique pour générer des vecteurs linéairement indépendants qui seront utilisés pour construire les matrices de projection de notre approche.

L'*instabilité des trajectoires* (ou sens) [Kappraff *et al.* 2005, Manneville 2005], causée par la propriété SIC, est l'une des caractéristiques de la théorie de chaos. Nous pouvons exploiter cette caractéristique pour générer plusieurs vecteurs qui sont linéairement indépen-

dants. Dans le cas de la suite logistique, si n vecteurs chaotiques sont générés en utilisant différentes valeurs de μ (de l'intervalle [3.5699456, 4]), chaque vecteur aura son propre sens. Par conséquent, cette famille de vecteurs est une famille linéairement indépendante.

Dans notre approche, nous utilisons la suite logistique pour générer de multiples vecteurs aléatoires. Ces vecteurs sont stockés dans une matrice 4D, appelée *Spiral Cube*, qui sera utilisée pour construire les matrices de projection. La Spiral Cube se compose de plusieurs *cellules* (matrice 3D carrée), chaque cellule contient plusieurs *boîtes*, et chaque boîte contient un vecteur chaotique généré en utilisant une valeur spécifique de μ qui appartient à l'intervalle [3.5699456, 4]. Il convient de mentionner que les vecteurs chaotiques sont stockés *spiralement* dans les cellules pour tromper l'adversaire si la Spiral Cube est volée (en ajoutant en même temps une autre alternative à la révocabilité de notre approche).

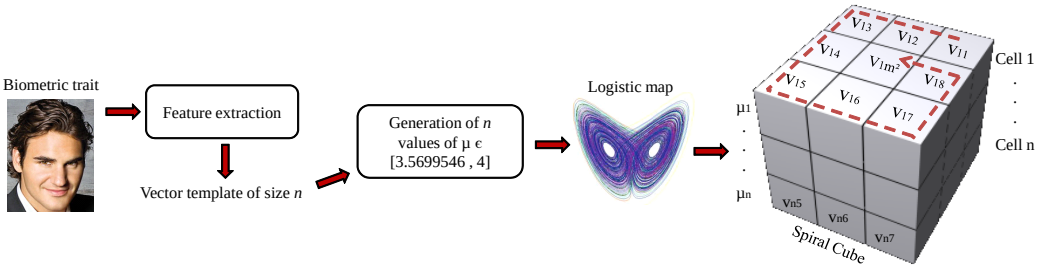


FIGURE 5.2 – Construction de Spiral Cube.

La construction de Spiral Cube dépend de la taille du modèle original non protégé (Figure 5.2). Supposons que le vecteur de caractéristique contient n valeurs, alors la Spiral Cube sera composée de n cellules et chaque cellule correspond à une valeur spécifique de μ (à savoir que les vecteurs de la même cellule sont générés en utilisant la même valeur de μ). Le nombre de vecteurs dans chaque cellule doit être supérieur ou égal à n et les cellules doivent être de forme carrée pour permettre de stocker *spiralement* les vecteurs chaotiques. Nous avons choisi de générer m^2 vecteurs chaotiques. m^2 est le premier nombre radical supérieur ou égal à n (m est le plus proche nombre entier supérieur ou égal à $\sqrt{n}$). Par conséquent, chaque cellule contient $m \times m$ boîtes, et chaque boîte contient un vecteur chaotique, de taille n, généré en utilisant la valeur de μ qui correspond à la cellule hôte.

5.2.3 Spiral Cube

Notre objectif est de construire une approche de transformation non inversible pour la protection des modèles biométriques qui répond à toutes les exigences de sécurité et de performance *sans avoir besoin d'une clé utilisateur*. Dans ce contexte, nous proposons un mécanisme non linéaire de projection aléatoire. L'approche proposée est applicable à tout système biométrique qui utilise des *vecteurs* de caractéristiques dans la tâche de classification. Nous décrivons ci-dessous les étapes principales de notre approche.

Tout d'abord, nous supposons que la base de données de formation contient x modèles, de taille n, appartiennent à z identités où chaque identité est représentée par y modèles, c'est-à-dire : $x = z \times y$. Lors de l'enrôlement, nous effectuons les étapes suivantes :

- Pour chaque modèle de formation T, nous calculons δ :

$$\delta = \frac{|max(T) - min(T)|}{m^2} \tag{5.2}$$

  - m est le plus proche nombre entier supérieur ou égal à $\sqrt{n}$.

- Ensuite, nous calculons le vecteur quantifié Q du modèle T :

$$Q_i = \begin{cases} 1 & \text{if } t_i = min(T) \\ m^2 & \text{if } t_i = max(T) \\ ceil\left(\dfrac{|T_i - min(T)|}{\delta}\right) & \text{else} \end{cases} \tag{5.3}$$

  - i ε [1,n].
  - Q_i ε [1, m^2].
  - $ceil(a)$ calcule le plus proche nombre entier supérieur ou égal à a.

- Pour chaque identité, on garde un seul vecteur quantifié (choisi de façon aléatoire parmi les y vecteurs qui correspondent à cette identité). Ensuite, nous obtenons une matrice qui contient les z vecteurs quantifiés choisis. Nous nous référons à cette matrice en utilisant le terme *Cube Map*.

- Pour chaque identité, nous construisons la matrice de projection en utilisant le Spiral Cube et la Cube Map (Figure 5.3). Nous utilisons les valeurs de vecteurs quantifiés (stockés dans la Cube Map) pour sélectionner les vecteurs chaotiques (stockés dans la Spiral Cube).
- Supposons que nous calculons la matrice de projection de l'identité numéro 1 en utilisant la Spiral Cube et Cube Map illustrées dans Figure 5.3. La première valeur du vecteur quantifié (premier vecteur de Cube Map correspond à l'identité 1) est associée à la première cellule dans le Spiral Cube, et ainsi de suite pour les autres valeurs de ce vecteur. Par exemple, si la première valeur est égale à 3, on extrait le vecteur numéro 3 de la première cellule dans le Spiral Cube. Si la dernière valeur est 5, on extrait le vecteur numéro 5 de la cellule numéro n (dernière cellule). Enfin, on obtient n vecteurs et on applique l'algorithme de Gram Schmidt pour construire la matrice de projection de l'identité numéro 1. Le même processus est appliqué pour calculer les matrices de projection des autres identités.
- Après le calcul de tous les modèles de références protégés, nous stockons ces modèles, Spiral Cube et Cube Map dans la base de données du système. Le stockage de Spiral Cube et Cube Map est publique.

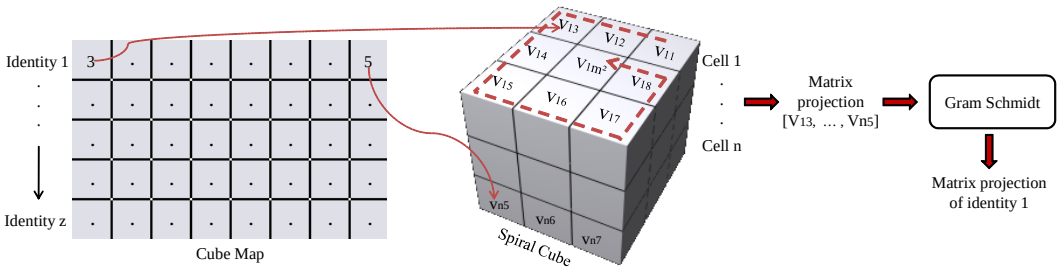


FIGURE 5.3 – Mécanisme de construction des matrices de projection.

Lors de l'authentification, le système protégé fonctionne comme suit :

- Pour chaque modèle de test, on applique les mêmes procédures d'extractions de caractéristiques et de quantification (relations 5.2 et 5.3) qu'on a appliqué sur les modèles de formation lors de l'étape de l'enrôlement.

- Nous utilisons un classifieur de type KNN pour identifier le vecteur le plus proche dans le Cube Map au modèle de test quantifié.
- Le vecteur le plus proche est utilisé pour construire la matrice de projection correspondant au vecteur de test, puis on calcule le modèle de test protégé.
- Le modèle de test protégé est comparé directement avec les modèles de formation protégés. La comparaison est réalisée en fonction du type de classificateur utilisé par le système visé.

La technique proposée est conforme aux exigences de la révocabilité, la diversité et la sécurité. Sachant que multiples acquisitions d'un même trait biométrique ne donnent pas généralement des ensembles de caractéristiques identiques, nous pouvons dire que le dynamisme de notre approche permet de créer des modèles biométriques différents pour une même identité dans la présence de ces variations. En outre, on peut protéger un modèle compromis en modifiant partiellement la Cube Map (par exemple, on peut modifier le vecteur quantifié correspondant à l'identité compromise, soit en refaisant la quantification ou en changeant partiellement ce vecteur quantifié). Ainsi, la révocabilité et la diversité sont assurées. Il convient de noter que la modification de Spiral Cube, ou l'ordre des cellules dans Spiral Cube, nécessite de refaire les étapes de la phase d'enrôlement, ce qui est un point faible de notre approche que nous comptons aborder dans les travaux futurs.

Pour la sécurité théorique de cette approche. Tout d'abord, nous analysons le scénario où l'adversaire a un accès au modèle protégé et à la Spiral Cube. Pour récupérer le modèle original non protégé, il faut trouver la matrice de projection utilisée durant la construction du modèle protégé. Dans ce scénario, il existe $(m^2 \times n)^n$ matrices de projection possibles. Par exemple, si n=100, alors le nombre de matrices possibles est 100^{200}, ce qui offre une grande robustesse contre les attaques à force brute. Supposons maintenant que l'adversaire a un accès au modèle protégé, à la Spiral Cube et à la Cube Map (toutes les données publiques). S'il ne connaît pas le rôle de Cube Map, le nombre de possibilités est similaire au scénario précédent (sécurité par obscurité). Si l'adversaire connait le rôle de Cube Map, le nombre de possibilités sera $(m^2 \times z)^n$, car il ne sait pas que les vecteurs de projection sont

stockés spiralement dans le Spiral Cube et il n'existe aucune preuve utile, dans la base de données ou dans les données publiques, pour déterminer la manière de stockage des vecteurs chaotiques. Alors selon cette complexité des attaques à force brute, nous pouvons dire que, même dans le pire des cas où l'adversaire a toutes les données publiques et le modèle protégé, la sécurité de notre système est suffisamment robuste à ces types d'attaques.

Cependant, comme nous avons dit dans le chapitre 4, en pratique, un adversaire peut exploiter la nature non uniforme des données biométriques pour lancer une attaque qui peut exiger beaucoup moins de tentatives pour atteindre la sécurité du système. Alors une analyse de sécurité rigoureuse est très nécessaire pour analyser correctement la sécurité des approches de protection des modèles biométriques. La performance, la diversité et la sécurité de l'approche proposée seront analysées encore plus rigoureusement dans la section suivante en utilisant les critères présentés dans le chapitre 4.

5.2.4 Expérimentations et discussion

5.2.4.1 Bases de données et procédures d'experimentation

Nous avons utilisé trois modalités et quatre bases de données dans cette expérimentation : les bases de données YALE et SHEFFIELD pour la reconnaissance de visage, la base de données PolyU FKP pour la reconnaissance des expressions de finger-knuckle et la base de données CASIA-Iris-Interval pour la reconnaissance d'iris.

FIGURE 5.4 – Exemples des images de la base de données Yale.

La base de données de visage YALE se compose de 165 images de visages qui appartiennent à 15 personnes distinctes (Figure 5.4). Cette base de données couvre une gamme mixte de la race, du sexe et de l'apparence. Les images sont caractérisées par des varia-

tions dans les expressions faciales et les conditions d'éclairage. Nous avons considéré 11 identités comme des utilisateurs légitimes et 4 identités comme des imposteurs. Chaque utilisateur légitime a été représenté par 5 images. Ainsi, notre ensemble d'apprentissage (formation) contient 55 modèles de références ; alors que notre ensemble de test contient 66 images. Chaque imposteur a la possibilité de lancer 11 attaques de fraude.

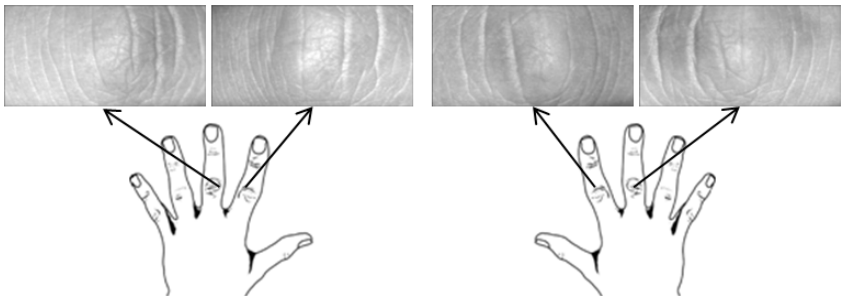


FIGURE 5.5 – Exemples des images de la base de données PolyU FKP.

La base de données PolyU FKP se compose de 7920 images des expressions de finger-knuckle de 165 personnes distinctes. L'idée de base derrière cette nouvelle modalité est d'utiliser la zone autour des phalanges du doigt comme un trait biométrique (Figure 5.5). Pour cette base de données, chaque personne est représentée par 48 images de 4 doigts (milieu / index de la main droite et milieu / index de la main gauche). Nous avons considéré 100 identités comme des utilisateurs légitimes et 65 identités comme des imposteurs. Chaque utilisateur légitime est représenté par 4 images. Ainsi, notre ensemble d'apprentissage contient 400 modèles de référence et l'ensemble de test contient 4400 images. Chaque imposteur a la possibilité de lancer 8 attaques de fraude.

La base de données CASIA-Iris-interval contient des images d'iris de 249 personnes distinctes (Figure 5.6). Nous ne gardons que 122 personnes qui ont des images d'iris des yeux gauche et droit à la fois. Nous construisons les modèles biométriques en utilisant la technique proposée dans [Masek & Kovesi 2003]. Nous avons considéré 100 identités comme des utilisateurs légitimes et 22 identités comme des imposteurs. Chaque utilisateur légitime a été représenté par deux images. Ainsi, notre ensemble d'apprentissage contient 200 modèles et l'ensemble de test contient 200 images. Chaque imposteur a la possibilité

de lancer deux attaques de fraude.

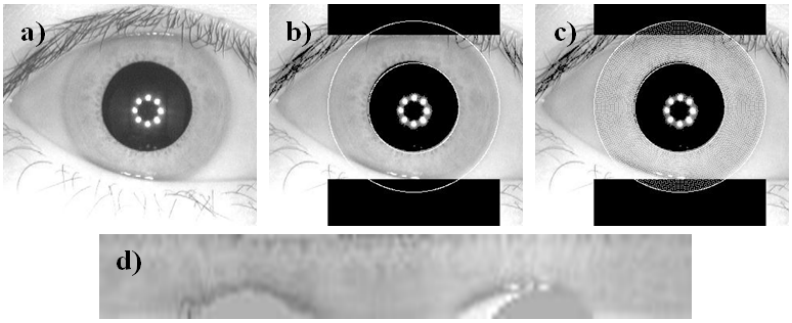


FIGURE 5.6 – a) Image d'iris de la base CASIA b) détection d'iris c) segmentation d) normalisation. Images générées en utilisant [Masek & Kovesi 2003]

La base de données de visage UMIST (appelée actuellement SHEFFIELD) se compose de 564 images de visages de 20 personnes des deux sexes et de diverses races. Chaque image d'une personne change l'angle à chaque prise par rapport à la vue frontale. Les angles de visages sont entre -30° et +90° (Figure 5.7). Notre objectif en utilisant la base de données SHEFFIELD est d'évaluer et de comparer la performance des systèmes de protection en présence de variations intra-sujets importantes. Pour la base de données SHEFFIELD, chaque personne était représentée par 6 images et une approche modifiée de *leave-one-out* a été utilisée pour les tests.

FIGURE 5.7 – Exemples des images de la base de données SHEFFIELD.

Pour chaque base de données, nous avons appliqué trois régimes de protection : Spiral Cube, Biohashing et BioPhasor. Les résultats ont été comparés et analysés en utilisant les critères présentés dans le chapitre 4. Le système biométrique utilisé dans notre expérimentation est basé sur la méthode d'extraction de caractéristiques *Laplacian Smoothing Transform* (LST) [Gu *et al.* 2010] (voir annexe A.4) et un classificateur de type KNN pour

la reconnaissance. La taille des modèles originaux et protégés est de 100.

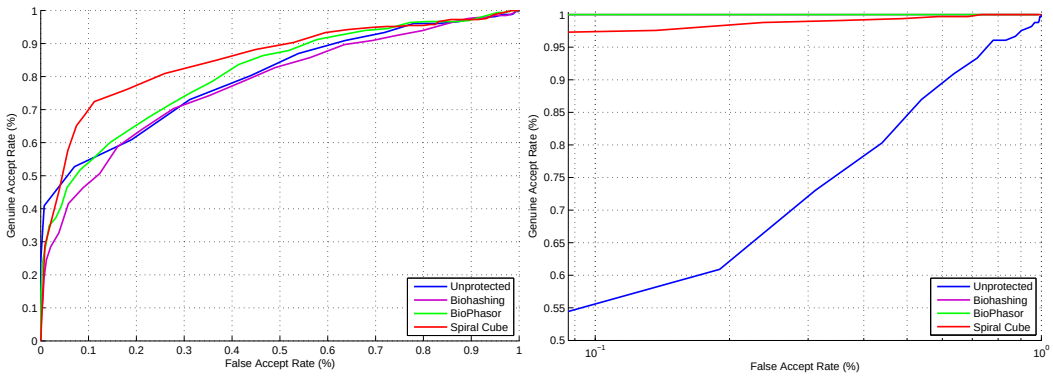
Il convient de noter que toutes méthodes d'extraction de caractéristiques peuvent être utilisées et testées dans cette expérimentation pour construire les modèles biométriques. Cependant, notre intérêt est d'évaluer l'effet des régimes de protection sur la performance plutôt que sur l'amélioration de performance. En particulier, notre intérêt, pour évaluer les performances à l'aide de modèles de grandes tailles (sous-section 5.2.4.6), nous a motivé à utiliser la technique LST. Contrairement aux méthodes traditionnelles, comme PCA et LDA, les exigences de calcul de LST ne sont pas étroitement liées à la dimensionnalité des données originales, mais dépendent plutôt du nombre de vecteurs propres de la matrice *Laplacienne* L_{MN} pour une image de taille M $\times$ N (voir l'annexe A.4 pour plus de détails).

5.2.4.2 Évaluation en utilisant la base de données YALE

La Figure 5.8 présente la courbe ROC du système non protégé ainsi que les courbes ROC des trois régimes de protection considérés dans cette étude. Tout d'abord, nous discutons le scénario de l'attaque à zéro effort (Figure 5.8(a)), où les paramètres de transformation sont connus par l'adversaire, qui essaie de contourner le système en utilisant leurs propres modèles biométriques. Une petite dégradation de performance peut être observée dans le cas de Biohashing tandis que la performance de classification est augmentée dans le cas de Biophasor et Spiral Cube. En pratique, les trois approches ont besoin d'informations supplémentaires (clé, mot de passe, Spirale Cube, Cube Map, etc.) lors de l'authentification. Dans le cas de Biohashing, la clé est utilisée sans traitement supplémentaire. Par contre, dans le cas de BioPhasor et Spiral Cube, même si l'adversaire possède des informations supplémentaires, des traitements supplémentaires sont nécessaires afin de d'exploiter les paramètres volés correctement / efficacement.

Dans le scénario où l'adversaire ne possède pas les paramètres de transformation (figure 5.8(b)), on observe une augmentation significative de la performance pour les trois systèmes protégés en comparaison avec le système non protégé. La réduction des FAR, dû à l'utilisation d'une clé spécifique pour chaque utilisateur, rend ce résultat très évident.

Nous pouvons également remarquer une petite dégradation des performances de l'approche Spiral Cube en comparaison avec les approches Biohashing et BioPhasor. Ceci peut être expliqué par les façons différentes dont l'information supplémentaire est utilisée.



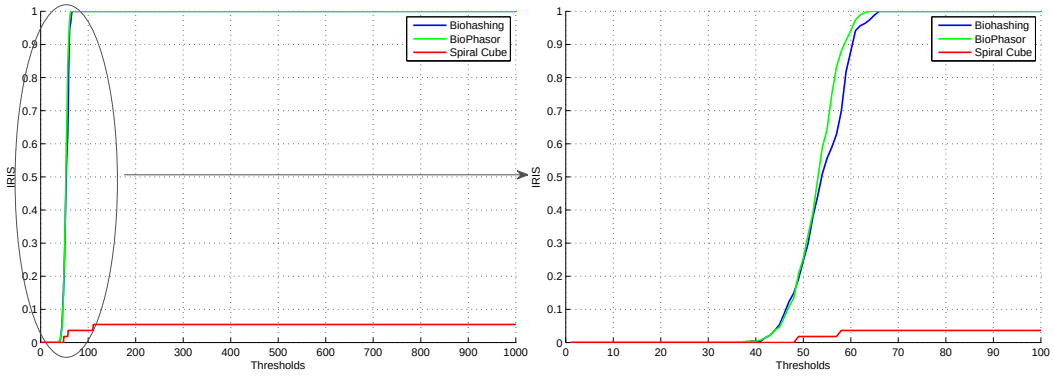
(a) Stolen parameters scenario (b) Unknown parameters scenario

FIGURE 5.8 – Courbes ROC en utilisant la base de données YALE.

Au moment de l'authentification, l'utilisateur est tenu de présenter sa clé dans les systèmes protégés par Biohashing et BioPhasor. Dans le cas de l'approche Spiral Cube, l'authentification se fait sans avoir besoin d'une clé utilisateur. Par conséquent, Biohashing et BioPhasor exigent une coopération de plus sur les utilisateurs, ce qui rend ces systèmes protégés semblables à ceux qui utilisent des mots de passe et des cartes d'identité (systèmes traditionnels). Ce caractère contraignant oblige la personne à se plier aux exigences techniques du procédé, ce qui constitue généralement un gage d'efficacité et d'acceptation. Dans ce contexte, nous pouvons dire que notre approche vise à assurer un équilibre entre la sécurité et la performance, mais aussi l'acceptation de l'utilisateur qui est une exigence des systèmes biométriques. Alors Spiral Cube s'avère bien adaptée pour faire face à cette limitation puisque la coopération des utilisateurs n'est pas exigée.

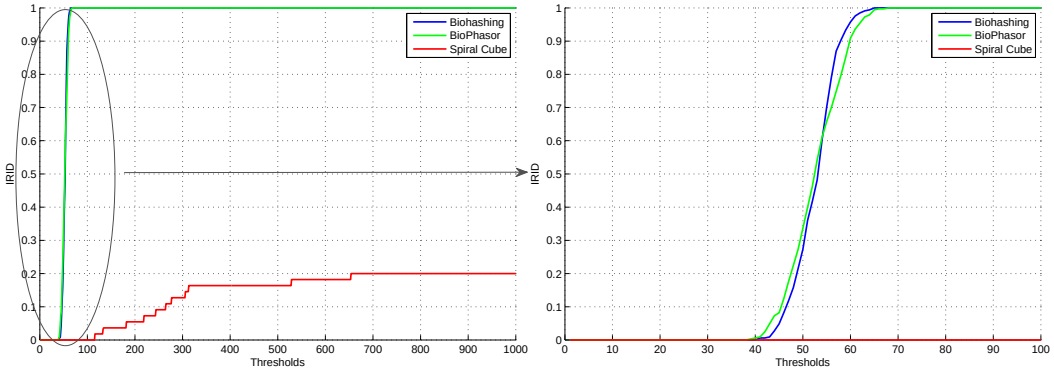
La Figure 5.9 présente les courbes IRIS des trois régimes de protection. Nous pouvons observer dans l'intervalle des seuils [0, 38] que les régimes de protection résistent à 100% contre les intrusions et l'inversion des modèles protégés. Biohashing et BioPhasor deviennent très vulnérables contre cette attaque dans l'intervalle [38, 62]. Par contre, Spiral Cube maintient une très faible IRIS, il est ainsi capable de résister contre l'intrusion

dans le même système. Après le seuil 65, le taux de réussite de l'attaque est de 100% pour Biohashing et BioPhasor. L'approche Spiral Cube conserve un taux de succès de 5,45%.



(a) 1000 thresholds (b) 100 thresholds

FIGURE 5.9 – Courbes IRIS en utilisant la base de données YALE.

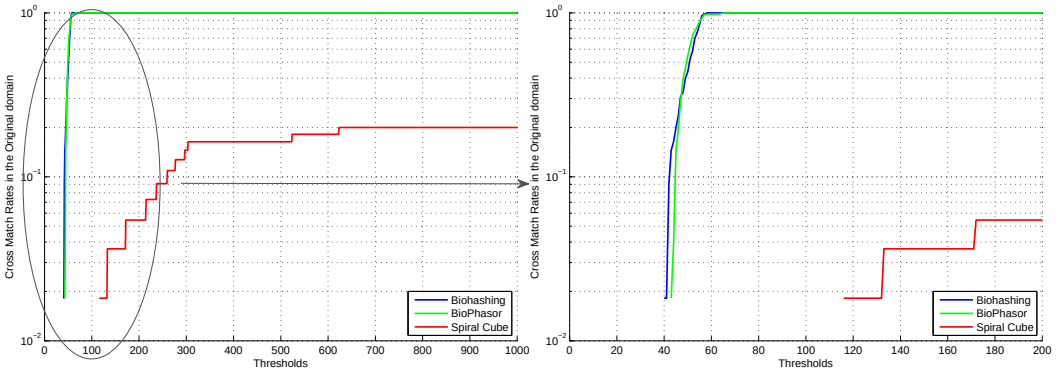


(a) 1000 thresholds (b) 100 thresholds

FIGURE 5.10 – Courbes IRID en utilisant la base de données YALE.

Pour les courbes IRID, nous discutons le scénario où l'intrusion est lancée dans un autre système contenant la même identité compromise (Figure 5.10). Les régimes Biohashing et BioPhasor résistent à 100% dans les 40 premiers seuils. Ensuite, IRID augmente rapidement et les systèmes protégés deviennent vulnérables à 100% au bout de la valeur de seuil 65. Pour Spiral Cube, l'attaque ne parvient pas à 100% jusqu'à ce que la valeur de seuil est de 120, elle conserve un taux de 20% de réussite, même après 1000 seuils. Ces résultats montrent clairement que le régime de protection Spiral Cube offre un niveau de sécurité très élevé par rapport à Biohashing et BioPhasor. Par conséquent, on peut conclure

qu'il fournit une haute non-inversibilité aux modèles biométriques.



(a) 1000 thresholds (b) 200 thresholds

FIGURE 5.11 – Courbes CMR_o en utilisant la base de données YALE.

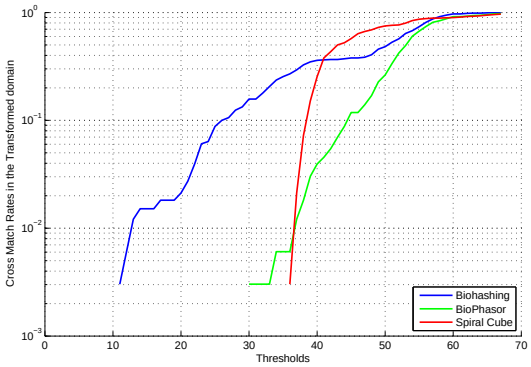


FIGURE 5.12 – Courbes CMR_t en utilisant la base de données YALE.

Les Figure 5.11 et 5.12 illustrent le succès de cross-matching de deux modèles protégés, qui appartiennent à la même identité, et qui sont volés de deux systèmes différents. Dans le domaine original (Figure 5.11), les deux modèles peuvent être facilement reliés après les valeurs de seuil 40 et 44 respectivement dans le cas de Biohashing et BioPhasor, ce qui est raisonnable comme nous l'avons déjà montré dans la Figure 5.9 (que l'inversion devient facile après ces valeurs de seuil). Le taux de réussite est de 100% après la valeur de seuil 55. Dans le cas de l'approche Spiral Cube, le taux de succès est de 0% jusqu'à le seuil 120 ; Spiral Cube conserve un taux de réussite de 20% même après 1000 seuils.

L'étude de cross-matching dans le domaine de la transformation (Figure 5.12) est très

utile pour mesurer la diversité des régimes de protection. Le taux de réussite est de 0% pour Biohashing, BioPhasor et Spiral Cube avant les valeurs seuil de 12, 30 et 37 respectivement. Après le seuil 37 pour Biohashing et 42 pour BioPhasor, jusqu'à la valeur de seuil 52, ces deux régimes sont plus résistants que Spiral Cube. Après le seuil 52, ils deviennent plus vulnérables que Spiral Cube.

Il convient de noter que l'inconvénient principal des approches de transformation non-inversibles est la difficulté de concevoir des techniques qui répondent à la discrimination, la diversité et la non-inversibilité simultanément. La discrimination est la capacité à minimiser les distances intra-sujets et augmenter les distances inter-sujets. Dans ce contexte, on peut expliquer les résultats de la Figure 5.12 comme suit. Spiral Cube a démontré une non-inversibilité élevée par rapport aux Biohashing et BioPhasor, ce qui justifie sa capacité d'être plus résistante contre la cross-matching dans le domaine original. Dans le domaine de transformation, les résultats sont assez similaires pour les trois approches étudiées. Généralement, l'approche Spiral Cube peut augmenter la non-inversibilité sans dégrader la diversité et la discrimination.

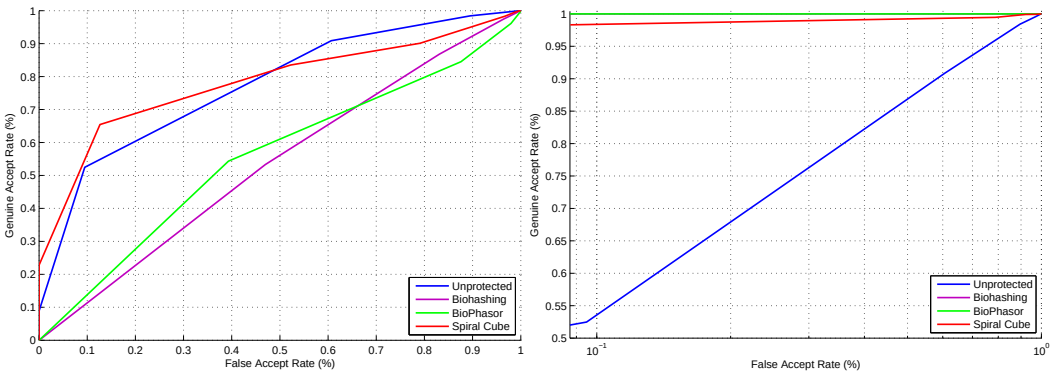
	EER		K-S test		Efficiency	
	S.P	U.P	S.P	U.P	S.P	U.P
Unprotected	28.85%		0.4613		———	
Biohashing	26.53%	0.27%	0.4285	0.9935	0.0527	0.9999
BioPhasor	25.93%	0.48%	0.4554	0.9927	0.1740	0.9998
Spiral Cube	21.58%	2.73%	0.6185	0.9686	0.2705	0.9574

TABLE 5.1 – Critères de convivialité / efficacité en utilisant la base YALE.

Le Tableau 5.1 présente plusieurs autres critères qui démontrent la robustesse de Spiral Cube et confirment les résultats des courbes de l'analyse de sécurité. Dans le scénario où les paramètres de transformation sont volés (SP), Spiral Cube offre les meilleures performances, diversité et efficacité. Dans le scénario où les paramètres de transformation sont inconnus (UP), les trois régimes ont des performances similaires, une petite dégradation peut être observée dans le cas de Spiral Cube en raison de notre intérêt de fournir la discrimination, la diversité, la non-inversibilité et l'acceptation de l'utilisateur simultanément.

5.2.4.3 Évaluation en utilisant la base de données PolyU FKP

Dans ce paragraphe, notre expérimentation est réalisée en utilisant une modalité caractérisée par des variations intra-sujets moyennes. Notre principal objectif est d'évaluer les schémas de protection en présence d'un nombre important d'identités. La Figure 5.13 présente la courbe ROC du système non protégé et les courbes ROC des trois régimes de protection considérés dans cette étude.



(a) Stolen parameters scenario (b) Unknown parameters scenario

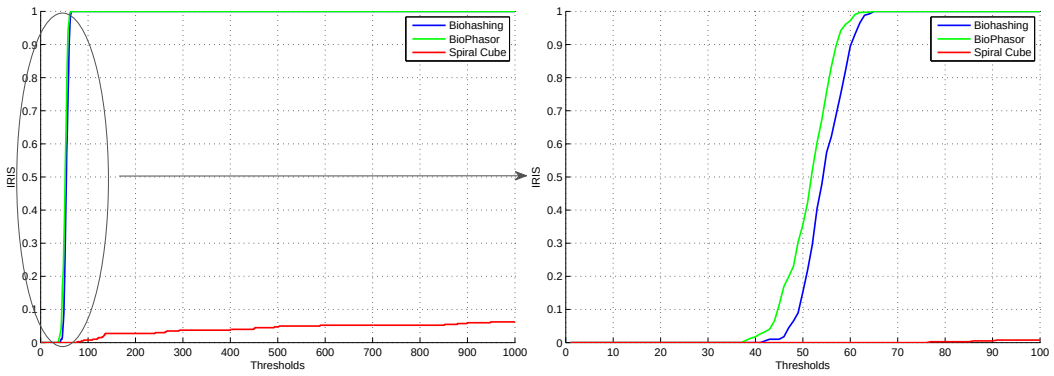
FIGURE 5.13 – Courbes ROC en utilisant la base de données PolyU FKP.

Dans le scénario d'une attaque à zéro effort où les paramètres de transformation sont connus par l'adversaire, et qui essaie de contourner le système en utilisant ses propres modèles biométriques (Figure 5.13(a)), nous pouvons observer une dégradation significative de la performance dans le cas de Biohashing et BioPhasor. Par contre, la performance de classification est augmentée dans le cas de Spiral Cube. En pratique, la présence de variations intra-sujets et un grand nombre d'identités peuvent aider l'adversaire à menacer la sécurité du système et à augmenter les chances de succès de l'attaque à zéro effort.

Dans le scénario où l'adversaire ne possède pas les paramètres de transformation (Figure 5.13(b)), on observe, comme dans le cas de la base de données YALE, une augmentation significative de la performance pour les trois systèmes protégés en comparaison avec le système non protégé. Cependant, cet avantage est perdu, pour Biohashing et BioPhasor, si les paramètres de transformation sont connus par l'adversaire.

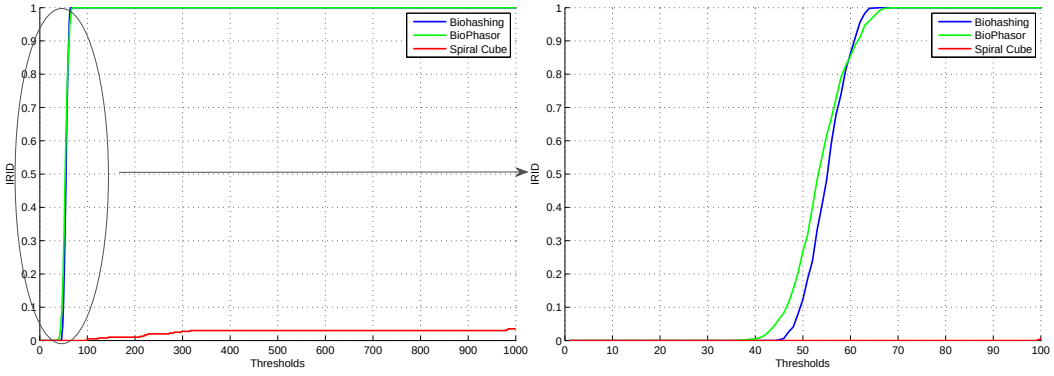
La Figure 5.14 illustre les courbes IRIS des trois régimes de protection. On peut obser-

ver que ces régimes résistent parfaitement à l'intrusion et l'inversion des modèles protégés dans l'intervalle de seuils [0, 40]. Biohashing et BioPhasor deviennent très vulnérables contre cette attaque dans l'intervalle [40, 65]. Contrairement à la série précédente d'expériences avec YALE, nous pouvons observer une légère dégradation de la résistance de BioPhasor par rapport à Biohashing, ce qui prouve l'efficacité de notre démarche d'optimisation proposée pour récupérer une approximation d'un modèle protégé par BioPhasor. Après la valeur de seuil 65, le taux de réussite de l'attaque devient 100% dans les systèmes protégés par Biohashing et BioPhasor. Spiral Cube maintient un taux de succès de 6,25%.



(a) 1000 thresholds (b) 100 thresholds

FIGURE 5.14 – Courbes IRIS en utilisant la base de données PolyU FKP.



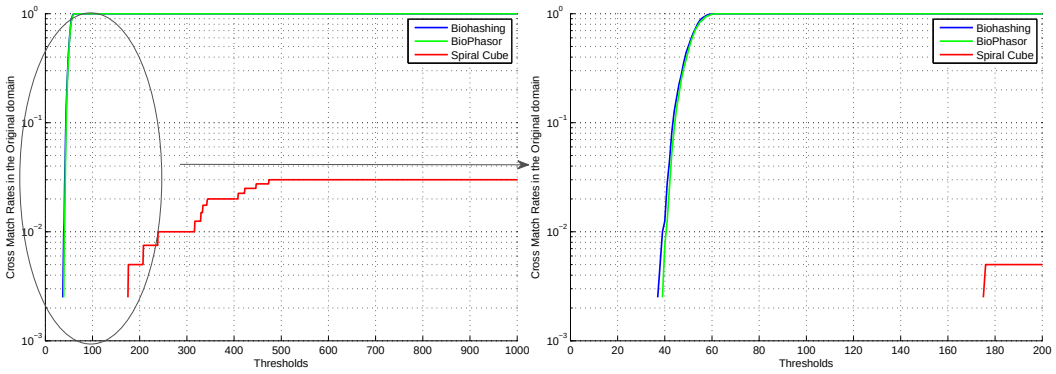
(a) 1000 thresholds (b) 100 thresholds

FIGURE 5.15 – Courbes IRID en utilisant la base de données PolyU FKP.

Dans le cas des courbes IRID (Figure 5.15), Biohashing et BioPhasor résistent à 100% respectivement dans les 46 et 40 premiers seuils. Ensuite, le taux de IRID augmente ra-

pidement et les systèmes protégés deviennent vulnérables à 100% au bout de la valeur de seuil 65. Pour Spirale Cube, l'attaque ne parvient pas à 100% jusqu'à ce que la valeur de seuil soit de 99, et il conserve un taux de réussite très faible de 3,5% (20% dans les expérimentations de YALE) même après 1000 seuils. Ces résultats montrent clairement que la sécurité de spirale Cube augmente considérablement si le nombre d'identités est grand comme nous l'avons montré théoriquement dans la section 5.2.3.

Les Figure 5.16 et 5.17 discutent la réussite de cross-matching de deux modèles protégés, d'une même identité, qui sont volés à partir de deux systèmes différents. Dans le domaine original (Figure 5.16), les résultats des approches Biohashing et BioPhasore sont très semblables à ceux obtenus en utilisant la base de données YALE. Pour l'approche Spiral Cube, le taux de réussite est de 0% jusqu'à la valeur seuil 174 et il est stable à 3% (20% dans les expérimentations de YALE) même après 1000 seuils. La résistance spirale Cube contre le cross-matching est significativement augmentée, par rapport aux expériences réalisées sur YALE, car l'inversion devient très difficile en présence d'un grand nombre d'identités.



(a) 1000 thresholds (b) 200 thresholds

FIGURE 5.16 – Courbes CMR_o en utilisant la base de données PolyU FKP.

Dans le domaine de la transformation (Figure 5.17), le taux de réussite de cross-matching est de 0% pour Biohashing, BioPhasor et Spiral Cube avant les valeurs de seuil 41, 36 et 39 respectivement. Après la valeur de seuil 40, Biohashing et BioPhasor sont plus résistants que Spiral Cube. Ensuite, après la valeur de seuil 54, ils deviennent plus vulnérables que Spiral Cube. Ces résultats montrent que Spiral Cube augmente la non-

inversibilité sans dégrader la diversité et la discrimination, même dans des systèmes qui contiennent un grand nombre d'identités.

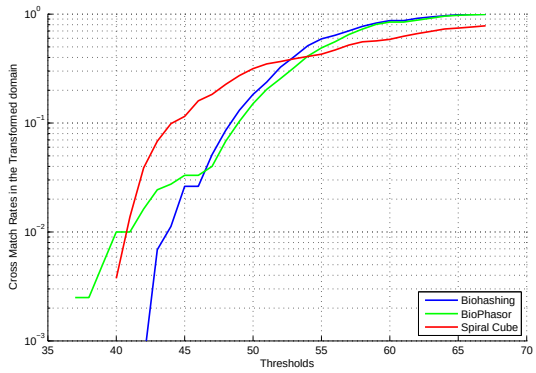


FIGURE 5.17 – Courbes CMR_t en utilisant la base de données PolyU FKP.

Le Tableau 5.2 présente les critères de performance, diversité et efficacité. Dans le scénario où les paramètres de transformation sont volés (SP), Biohashing et BioPhasor perdent totalement l'efficacité. En outre, nous pouvons observer une dégradation significative de la diversité et de la performance pour Biohaching. Par contre, Spirale Cube conserve des valeurs très acceptables pour tous les critères. Dans le scenario où les paramètres de transformation sont inconnus (UP), les trois régimes ont des performances similaires. Une petite dégradation de performance peut être remarquée dans le cas de Spiral Cube en raison de notre intérêt de fournir simultanément la discrimination, la diversité et la non-inversibilité.

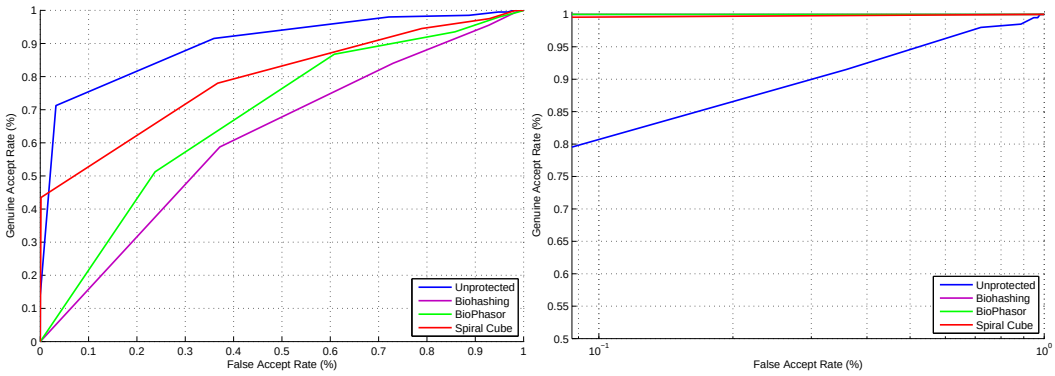
	EER		K-S test		Efficiency	
	S.P	U.P	S.P	U.P	S.P	U.P
Unprotected	31.22%		0.4624		———	
Biohashing	46.84%	1%	0.0633	0.9948	-1.0427	0.9903
BioPhasor	43.23%	2%	0.0736	0.9900	-0.9581	0.9802
Spiral Cube	27.68%	3.35%	0.6857	0.8007	0.0419	0.9520

TABLE 5.2 – Critères de convivialité / efficacité en utilisant la base PolyU FKP.

5.2.4.4 Évaluation en utilisant la base de données CASIA

Dans cette série d'expériences, nous avons choisi d'évaluer un système biométrique de reconnaissance d'iris. Cette modalité permet, malgré les erreurs lors de l'extraction d'un iris à partir des images de l'œil, une fiabilité parfaite et une haute unicité (c'est-à-dire, la probabilité de trouver deux iris identiques est de 10^{-72} selon [Daugman 2004]). La conception d'un système robuste nécessite de représenter chaque classe (identité) par *plusieurs* modèles d'iris. Notre objectif dans cette section est d'évaluer les systèmes de protection dans un système contenant un grand nombre d'identités où chaque identité est représentée seulement par deux modèles (extraits à partir de l'iris gauche et l'iris droit).

Dans le scénario de l'attaque à zéro effort (Figure 5.18(a)), lorsque les paramètres de transformation sont connus par l'adversaire, la performance des trois systèmes protégés est considérablement dégradée par rapport au système non protégé. Cependant, Spiral Cube possède les meilleures performances avec une dégradation de 10,14% (voir le Tableau 5.3). L'augmentation de la FRR, qui est principalement due au nombre faible des modèles de références pour chaque identité, justifie ce résultat.

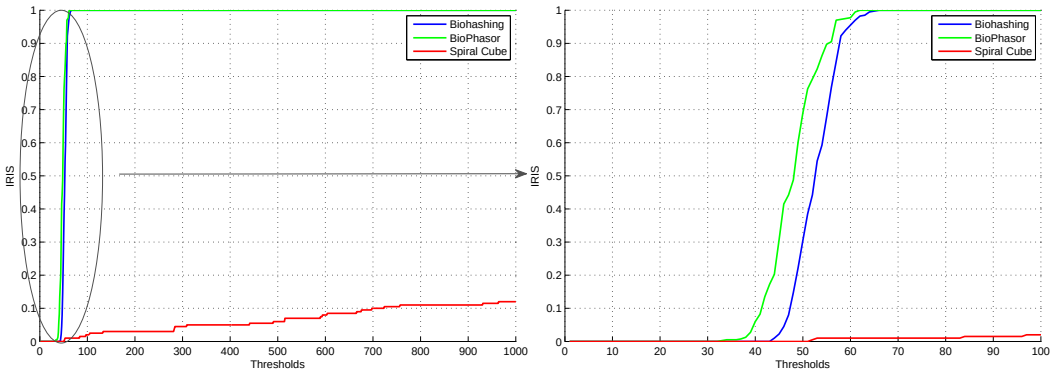


(a) Stolen parameters scenario (b) Unknown parameters scenario

FIGURE 5.18 – Courbes ROC en utilisant la base de données CASIA.

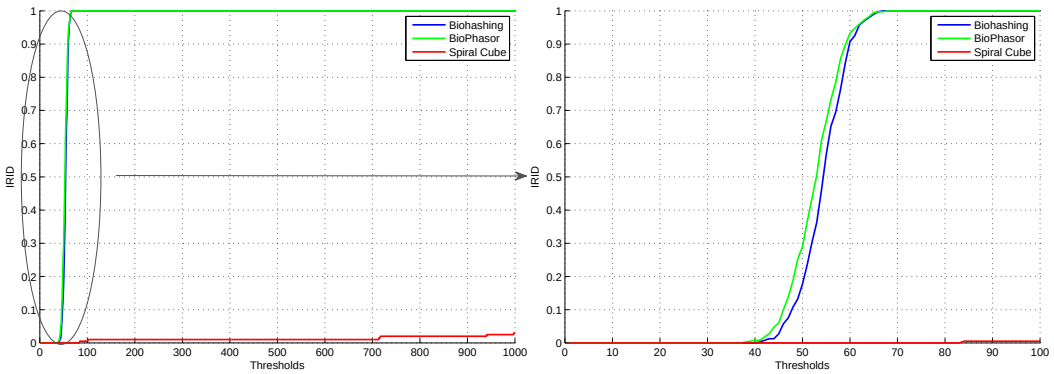
Dans le scénario où l'adversaire ne possède pas les paramètres de transformation (Figure 5.18(b)), nous pouvons observer, comme dans les expérimentations de Yale et PolyU FKP, une augmentation significative de performance pour les trois systèmes protégés par rapport au système non protégé.

La Figure 5.19 présente les courbes IRIS des trois régimes de protection. Biohashing et BioPhasor résistent à 100% dans les 43 et 32 premiers seuils respectivement. Ensuite, le taux de IRIS augmente rapidement et les deux systèmes protégés deviennent vulnérables à 100% au bout de la valeur de seuil 65. L'approche Spiral Cube conserve un taux de succès de 12% (6,25% dans le cas de PolyU FKP), ce qui confirme que la conception des systèmes non protégés influence l'efficacité des régimes de protection.



(a) 1000 thresholds (b) 100 thresholds

FIGURE 5.19 – Courbes IRIS en utilisant la base de données CASIA.

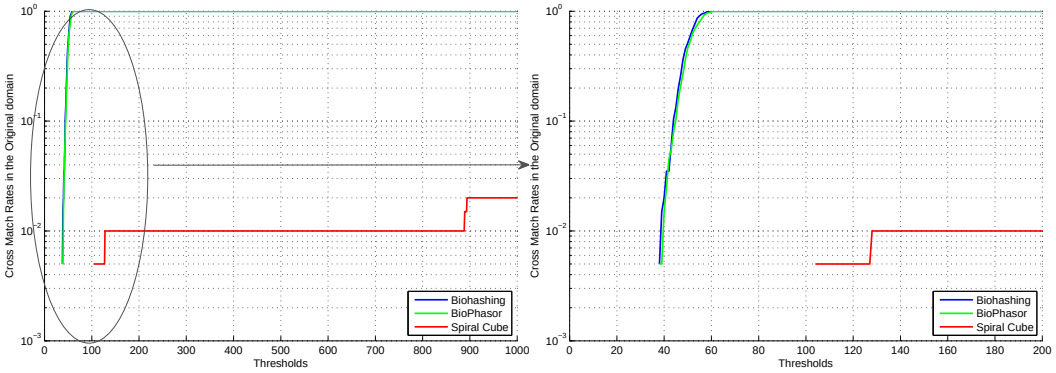


(a) 1000 thresholds (b) 100 thresholds

FIGURE 5.20 – Courbes IRID en utilisant la base de données CASIA.

Dans le cas des courbes IRID (Figure 5.20), le système non protégé a cette fois un effet opposé sur une attaque d'intrusion en utilisant un modèle biométrique volé à partir d'un système biométrique différent. Spiral Cube conserve un taux de réussite très faible de 2,5% (de 20% et de 3,5% pour les expériences de Yale et PolyU FKP respectivement) même

après 1000 seuils. Si chaque identité est représentée par un nombre faible de modèles de référence dans le système, l'attaque IRID devient plus difficile pour un adversaire.



(a) 1000 thresholds (b) 200 thresholds

FIGURE 5.21 – Courbes CMR_o en utilisant la base de données CASIA.

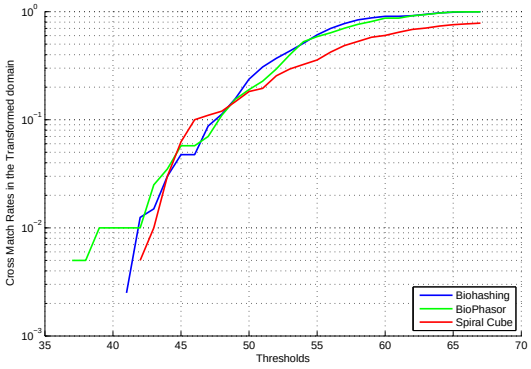


FIGURE 5.22 – Courbes CMR_t en utilisant la base de données CASIA.

Les Figures 5.21 et 5.22 illustrent le succès de la liaison de deux modèles protégées, qui appartiennent à la même identité, et qui sont volés à partir de deux systèmes différents. Dans le domaine original (Figure 5.21), les résultats des régimes sont relativement similaires à ceux obtenus en utilisant la base de données PolyU FKP. Une petite dégradation peut être observée dans le cas de Spiral Cube (le taux de réussite est de 0% pour les 100 premiers seuils dans la base de données CASIA-iris et 0% pour les 174 premiers seuils de la base de données PolyU FKP) en raison de la dégradation d'IRIS qui est principalement due à la conception de systèmes non protégés dans notre expérimentation avec CASIA.

Dans le domaine de la transformation (Figure 5.22), le taux de réussite est de 0% pour Biohashing, BioPhasor et Spiral Cube avant respectivement les valeurs de seuil 40, 36 et 31. Après la valeur de seuil 50, Biohashing et BioPhasor sont plus vulnérables que Spiral Cube. Par conséquent, on peut dire que l'équilibre entre la non-inversibilité, la diversité et la discrimination est toujours maintenu par Spiral Cube.

	EER		K-S test		Efficiency	
	S.P	U.P	S.P	U.P	S.P	U.P
Unprotected	19%		0.7224		———	
Biohashing	39.56%	1%	0.1201	0.9974	-2.7847	0.9755
BioPhasor	36.53%	0.98%	0.1742	0.9933	-2.1380	0.9785
Spiral Cube	29.14%	4.92%	0.5806	0.8260	-1.0460	0.9070

TABLE 5.3 – Critères de convivialité / efficacité en utilisant la base CASIA.

Le Tableau 5.3 confirme les résultats des courbes analytiques. Dans le scénario où les paramètres de transformation sont volés (SP), la performance des trois régimes de protection est dégradée par rapport au système non protégé et l'efficacité est perdue en raison de la conception *incohérente* du système non protégé. Spiral Cube offre les meilleures performances en termes de critères considérés. Dans le scenario où les paramètres de transformation sont inconnus (UP), les trois régimes de protection ont des performances similaires et les valeurs de tous les critères sont bien acceptables.

5.2.4.5 Évaluation en utilisant la base de données UMIST

Le but de cette sous-section est d'étudier la sécurité des systèmes biométriques en présence des variations intra-sujets importantes (c'est-à-dire, variation de pose de visage dans notre cas). En outre, nous nous efforçons d'étudier la sécurité dans un système qui utilise des modèles biométriques de petites tailles et qui contient un petit nombre d'identités (parce que nous avons déjà montré que la sécurité de spirale Cube est améliorée grâce à l'augmentation du nombre d'identités et de la taille du modèle). Ainsi, cette expérience a pour objectif d'évaluer la sécurité de Spiral Cube dans des conditions non idéales.

Pour la base de données UMIST, nous avons adopté une approche *leave-one-out* mo-

difiée afin d'évaluer les trois régimes de protection. Dans ce contexte, chaque algorithme est exécuté N fois. Pour chaque itération, N-1 modèles de référence sont utilisés pour la formation et le modèle restant est censé être comme un modèle volé du système. L'adversaire essaie de récupérer le modèle original (nous supposons qu'il connaît les paramètres de transformation du modèle volé). Ensuite, l'approximation calculée est utilisée pour accéder au système. Si l'adversaire est accepté, le succès de l'attaque de cette itération est de 100%, sinon il est de 0%. Le succès global de la réussite de cette attaque est la moyenne de toutes les N itérations.

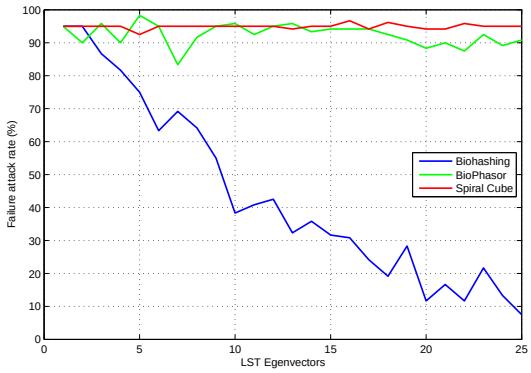
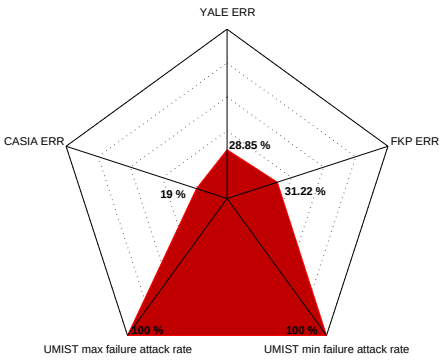


FIGURE 5.23 – Taux d'échec de l'attaque proposée.

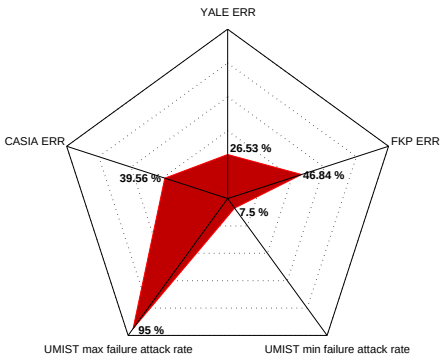
La Figure 5.23 présente les résultats des trois régimes de protection. Nous observons que Biohashing est très vulnérable dans ces conditions de test, un adversaire peut facilement menacer la sécurité. Spiral Cube et BioPhasor ont prouvé une grande non-inversibilité même lorsque le nombre d'identités est faible et les modèles biométriques sont de petites tailles. Spiral Cube a montré plus de résistance par rapport à BioPhasor. Par conséquent, la sécurité de notre approche est suffisamment robuste contre les attaques possibles même dans des conditions de test non idéales.

La Figure 5.24 résume les résultats des trois régimes de protection dans le cas où la taille des modèles originaux et protégés est de 100. Pour le EER, nous avons considéré seulement le scénario où les paramètres de transformation sont connus par l'adversaire. La Figure 5.24(a) illustre les résultats désirés dans un schéma de protection idéal qui est en

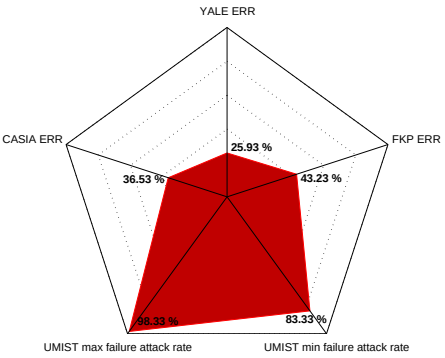
mesure de maintenir, au moins, le EER du système non protégé et qui résiste à 100% contre les attaques possibles. Pour la base de données YALE, qui se caractérise par des variations intra-sujet négligeables et un nombre limité d'identités, les trois approches fournissent la performance requise et Spiral Cube a la meilleure performance. Pour la base de données FKP, qui se caractérise par des variations intra-sujets moyennes et un grand nombre d'identités, nous pouvons observer une dégradation significative de la performance dans le cas de Biohashing et BioPhasor. Spiral Cube augmente la performance du système non protégé. Dans le cas de la base de données CASIA, où la conception du système non protégé n'est pas optimale, les performances des trois régimes de protection sont dégradées. Dans le cas de la base de données SHEFFIELD, BioPhasor et Spiral Cube ont prouvé un haut niveau de sécurité, Biohashing est très vulnérable dans ces conditions d'expérimentation. En bref, Spirale Cube est le plus proche au régime de protection idéal.



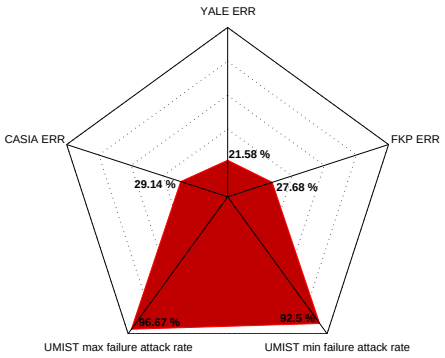
(a) Régime de protection idéal



(b) Biohashing



(c) BioPhasor



(d) Spiral Cube

FIGURE 5.24 – Illustration des résultats des régimes de protection.

Dans les expérimentations précédentes, l'évaluation de la performance et la comparaison de Spiral Cube avec Biohashing et BioPhasor ont été réalisées en utilisant une taille de modèle égale à 100. La sous-section suivante vise à étendre nos expériences sur YALE, FKP et CASIA en utilisant des modèles originaux et protégés de différentes tailles.

5.2.4.6 Performance avec des modèles de grandes tailles

Le Tableau 5.4 illustre les critères de performance, diversité et efficacité des trois schémas de protection dans le cas des bases YALE, FKP et CASIA en utilisant des modèles de tailles différentes, y compris trois grandes tailles. Dans notre évaluation, nous avons considéré seulement le scénario où les paramètres de transformation sont connus par l'adversaire. Lorsque les paramètres de transformation sont inconnus, nous avons déjà montré que tous les critères d'évaluation pour les trois régimes de protection s'améliorent considérablement indépendamment des conditions d'évaluation.

Pour la base de données de YALE, Biohashing et BioPhasor conservent la performance et la diversité du système non protégé, mais leur efficacité diminue en utilisant des tailles de modèles égalent à 10 et 50 pour les deux approches et aussi les tailles de modèles 250 et 500 dans le cas de Biohashing. Spiral Cube améliore la performance et maintient la diversité / efficacité du système non protégé dans les différentes tailles des modèles. Pour la base de données FKP, nous pouvons observer une dégradation des performances / diversité pour Biohashing et BioPhasor. En outre, l'efficacité est perdue dans les différentes tailles des modèles. Spiral Cube fournit des valeurs très acceptables pour tous les critères (sauf pour l'efficacité des modèles de tailles 10 et 500). Dans le cas de la base de données CASIA, la performance / diversité des trois régimes de protection sont dégradées tandis que l'efficacité est perdue pour la plupart des tailles de modèles. Cependant, malgré que la conception de système non protégé est non optimale, nous pouvons observer que Spiral Cube fournit des valeurs acceptables pour tous les critères dans le cas de la taille du modèle qui est égale à 250. En général, les résultats du Tableau 5.4 sont en accord avec les résultats présentés dans les sous-sections précédentes. Spiral Cube offre la meilleure performance,

diversité et efficacité. En général, nous pouvons conclure que l'efficacité des régimes de protection est bien influencée par la conception du système non protégé, la présence de variations intra-sujets et le nombre d'identités.

		YALE			FKP			CASIA		
Size	Protection Approach	EER	K-S test	Efficiency	EER	K-S test	Efficiency	EER	K-S test	Efficiency
10	Unprotected	32.48%	0.4344	———	40.96%	0.5745	———	33.53%	0.6647	———
	Biohashing	36.87%	0.2893	-0.0386	48.94%	0.0389	-0.3756	45.23%	0.1423	-0.6265
	BioPhasor	37.08%	0.2607	-0.1315	48.85%	0.0408	-0.3724	44.68%	0.1211	-0.5649
	Spiral Cube	22.79%	0.4785	+0.3142	42.30%	0.2415	-0.1820	37.36%	0.2524	-0.2670
50	Unprotected	30.34%	0.4691	———	31.76%	0.5459	———	20.13%	0.7532	———
	Biohashing	32.41%	0.3530	-0.2549	47.82%	0.0627	-1.1666	41.67%	0.1786	-2.6809
	BioPhasor	29.70%	0.4390	-0.0695	47.79%	0.0597	-1.1713	43.18%	0.6450	-2.8618
	Spiral Cube	21.03%	0.5541	+0.2762	24.73%	0.7016	+0.1187	36.95%	0.5507	-1.8250
100	Unprotected	28.85%	0.4613	———	31.22%	0.4624	———	19%	0.7224	———
	Biohashing	26.53%	0.4285	+0.0527	46.84%	0.0633	-1.0427	39.56%	0.1201	-2.7847
	BioPhasor	25.93%	0.4554	+0.1740	43.23%	0.0736	-0.9581	36.53%	0.2624	-2.1380
	Spiral Cube	21.58%	0.6185	+0.2705	27.68%	0.6857	+0.0419	29.14%	0.5806	-1.0460
250	Unprotected	29.07%	0.9498	———	34.54%	0.3522	———	18.48%	0.6796	———
	Biohashing	28.85%	0.4968	-0.0202	45.12%	0.1307	-0.4959	36.68%	0.2672	-1.9708
	BioPhasor	24.18%	0.5262	+0.2035	46.92%	0.0647	-0.5719	34.67%	0.1783	-1.6197
	Spiral Cube	21.36%	0.5460	+0.2729	27.37%	0.7580	+0.3405	15.38%	0.8191	+0.1228
500	Unprotected	28.65%	0.9577	———	38.27%	0.2660	———	19.96%	0.6474	———
	Biohashing	29.51%	0.4218	-0.0775	44.26%	0.1157	-0.2740	33.75%	0.3250	-1.3152
	BioPhasor	25.87%	0.5183	+0.1604	46.55%	0.0694	-0.3588	37.33%	0.2062	-1.5129
	Spiral Cube	24%	0.4001	+0.1266	38.12%	0.3903	-0.0238	30.93%	0.6231	-0.8046
1000	Unprotected	28.74%	0.8601	———	40.79%	0.2154	———	23.66%	0.5578	———
	Biohashing	27.55%	0.4573	+0.0267	39.68%	0.1180	+0.0347	28.91%	0.3756	-0.2825
	BioPhasor	23.89%	0.5452	+0.2034	45.57%	0.0798	-0.1793	39.69%	0.1955	-1.0498
	Spiral Cube	18.73%	0.5920	+0.4422	42.62%	0.7269	+0.0044	27.60%	0.7501	-0.1817

TABLE 5.4 – Critères de convivialité / efficacité en utilisant des modèles biométriques de différentes tailles.

5.3 Fingerprint Shell pour la protection des minuties

5.3.1 Introduction

L'empreinte digitale est une modalité biométrique populaire qui est largement utilisée dans de nombreuses applications pour l'authentification des personnes, elle offre une haute diversité et une performance acceptable. Les empreintes digitales ne changent pas tout au

long de la vie d'une personne, sauf pour des accidents tels que des ecchymoses et des coupures sur les doigts. Cette propriété rend les empreintes digitales une modalité biométrique très attrayante pour les systèmes biométriques commerciaux (ATM, Smartphone, Credit Card, E-Commerce, etc.) et gouvernementaux (Carte d'identité nationale, identification des criminels, passeport biométrique, etc.).

Bien que des systèmes très efficaces sont actuellement disponibles, la reconnaissance des empreintes digitales ne peut pas être considérée comme un problème complètement résolu en terme de performance et précision [Maltoni *et al.* 2009], sans oublier tous les défis de sécurité et de vie privée (Chapitre 2). La plupart des systèmes de reconnaissance des empreintes digitales utilisent des représentations (modèles biométriques) basées sur les minuties. Cependant, plusieurs études ont prouvé que l'impression originale d'une empreinte digitale peut être reconstruite à partir des informations fournies par ses minuties [Ross *et al.* 2005, Ross *et al.* 2007, Cappelli *et al.* 2007, Galbally *et al.* 2010, Li & Kot 2012], ce qui rend le problème d'assurer la sécurité de cette modalité très critique. Comme nous avons vu dans le Chapitre 3, selon la nature des fonctions de transformation, nous pouvons diviser les approches de transformation de caractéristiques en deux classes : Biohashing et transformation non inversible. Cependant, une autre classification de ces approches peut être considérée. Selon la forme du modèle original, les régimes de transformation peuvent être divisés en deux catégories principales : approches basées sur les *vecteurs* [Moujahdi *et al.* 2012] et approches basées sur les *points d'intérêts* [Ratha *et al.* 2007] (principalement conçues pour les systèmes basés sur les minuties).

Dans cette thèse, nous présentons une nouvelle approche pour la protection des modèles des empreintes digitales appelée *Fingerprint Shell*. Cette technique peut être considérée comme une approche de transformation de caractéristiques non inversible basées sur les *points d'intérêts* qui répond aux exigences de révocabilité, diversité, sécurité et performance. Dans ce contexte, on a exploité les informations fournies par les minuties pour construire une nouvelle représentation sous forme de courbes spirales spéciales, qui peuvent être utilisées directement dans la tâche de reconnaissance au lieu de la représen-

tation traditionnelle basée sur les minuties. Bien que la nouvelle approche répond à toutes les exigences, sa performance est moins sensible à la translation / rotation des empreintes digitales (par rapport aux systèmes traditionnels) et elle est suffisamment robuste contre les attaques à force brute et les attaque à zéro effort.

Le reste de la section est organisé comme suit. Dans la sous-section 5.3.2, les principes de base des systèmes de reconnaissance des empreintes digitales sont abordés. La sous-section 5.3.3 présente un survol sur les approches de protection des empreintes digitales. La sous-section 5.3.4 détaille le fonctionnement de l'approche proposée. Nos résultats expérimentaux, les comparaisons et la discussion sont présentés dans la section 5.3.5.

5.3.2 Reconnaissance des empreintes digitales

La reconnaissance des empreintes digitales, qui est basée sur l'utilisation des minuties (Figure 5.25), se déroule suivant trois étapes : 1) pré-traitement des impressions ; 2) Extraction des points d'intérêts (minuties) ; 3) comparaison. Chacune de ces étapes se déroule également suivant plusieurs démarches.

Pour les étapes générales (partagées par la plupart des travaux) du prétraitement des impressions des empreintes digitales. 1) Il faut appliquer une segmentation sur les images envoyées par le capteur pour isoler l'impression qui contient les informations biométriques du fond (qui est bruyant). La procédure de segmentation consiste généralement sur la division de l'image en plusieurs blocs, ensuite le calcul de la variance du gradient pour chaque bloc, et enfin la comparaison de variance avec un seuil prédéterminé pour décider si le bloc est utile ou non. 2) Calculer l'orientation du pixel du centre de chaque bloc pour générer le domaine de l'orientation de l'impression. 3) Estimation de la fréquence de crêtes de la peau en utilisant une fonction d'approximation sinusoïdale. 4) Filtrage par Gabor. 5) Binarisation. 6) Extraction de squelette de l'impression.

Pour l'extraction des points d'intérêts, une fois que le squelette est obtenu, un balayage simple (par exemple en utilisant une fenêtre de taille 3×3) permet la détection de pixels qui correspondent à des terminaisons et des bifurcations, qui présentent des minuties.

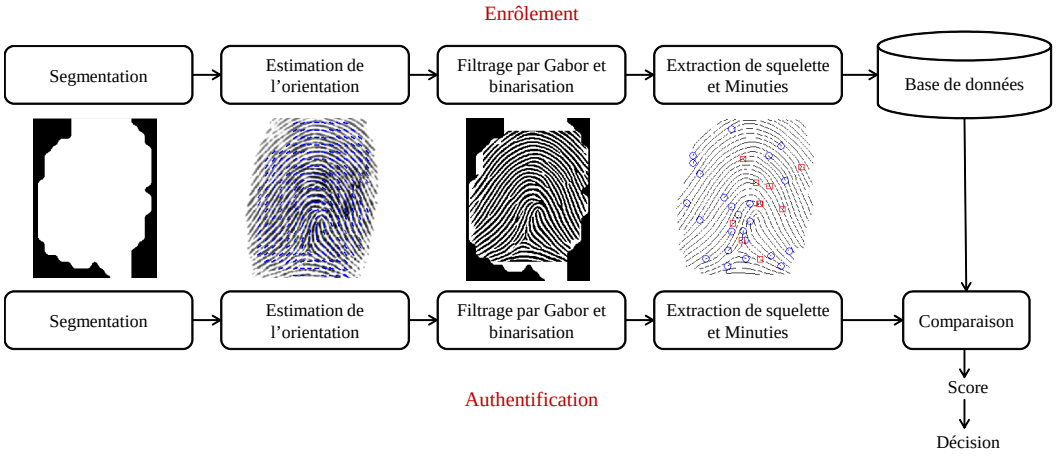


FIGURE 5.25 – Fonctionnement général d'un système de reconnaissance des empreintes digitales basé sur l'utilisation des minuties.

Pour la comparaison de deux ensembles de minuties, il y a plusieurs techniques en littérature. Toutes ces techniques partagent en général deux étapes principales (Figure 5.26) : 1) appliquer deux alignements pour minimiser la translation et la rotation (qui présentent les variations intra-sujets de cette modalité) des impressions et maximiser par conséquent le nombre des minuties qui se correspondent. 2) Calculer le score de correspondance qui est égal au nombre des minuties qui se correspondent divisé par le nombre total des minuties.

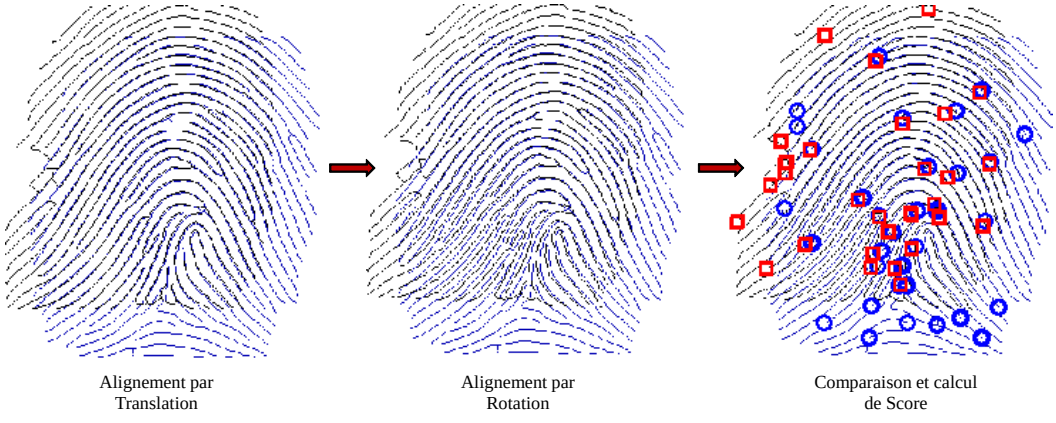


FIGURE 5.26 – Exemple de l'implémentation de la méthode de comparaison proposée dans [Kryszczuk *et al.* 2004].

Pour plus de détails concernant les différentes méthodes de la reconnaissance des em-

preintes digitales, vous pouvez consulter [Maltoni *et al.* 2003, Maltoni *et al.* 2009].

Ce type de systèmes nécessite le stockage des informations fournies par les minuties (coordonnées et orientations) dans la base de données. Cependant, plusieurs travaux [Ross *et al.* 2007, Cappelli *et al.* 2007, Galbally *et al.* 2010, Li & Kot 2012], ont prouvé que l'impression d'empreintes digitales peut être reconstruite à partir de ces informations minuties. Ainsi, la conception de nouvelles solutions de protection et de nouvelles représentations sécurisées pour cette modalité devient de plus en plus importante.

5.3.3 Travaux connexes

Dans la pratique, les variations intra-sujets rendent la reconnaissance d'empreintes digitales une tâche extrêmement difficile, parce que plusieurs acquisitions du même doigt sont très peu probables d'aboutir à un ensemble identique de minuties. Les principaux facteurs responsables des variations intra-sujets sont dus à la distorsion non-linéaire (en raison de l'élasticité de la peau), la translation et la rotation d'une impression (Figure 5.27). Un doigt peut être placé et / ou mis en rotation sur le capteur différemment pendant plusieurs authentifications (selon [Maltoni *et al.* 2009], le déplacement de 2 mm correspond à 40 pixels de translation et $\pm 20^{\circ}$ de rotation peut être observé). Par conséquent, la reconnaissance des empreintes digitales est très sensible à l'orientation et à la translation des impressions, ce qui rend la protection des modèles de cette modalité encore plus compliquée.

Plusieurs approches basées sur les *vecteurs* [Teoh *et al.* 2007, Moujahdi *et al.* 2012] ont été appliquées pour la protection des empreintes digitales. L'idée principale de ces régimes est de construire des vecteurs de caractéristiques en utilisant la texture globale des impressions. Cependant, les images d'empreintes digitales sont principalement traitées, dans la plupart des applications, en utilisant une représentation basée sur des points d'intérêt (représentation par minuties), ce qui nécessite des techniques de protection appropriées à cette représentation. Nous pouvons diviser les approches de protection basées sur des *points d'intérêt* en trois catégories.

Tout d'abord, les techniques qui transforment la représentation de minuties à une repré-

FIGURE 5.27 – Exemples de translation et rotation de deux impressions d'un même doigt (images prises de [Jain *et al.* 2008, Uz *et al.* 2009]).

sentation vectorielle [Farooq *et al.* 2007, Tulyakov *et al.* 2007, Ahn *et al.* 2008, Kumar *et al.* 2010, Li *et al.* 2010]. Par exemple, dans [Farooq *et al.* 2007], les informations fournies par plusieurs triplets de minuties sont utilisées pour générer un histogramme binarisé. La clé utilisateur est utilisée pour randomiser l'histogramme et obtenir le vecteur binaire protégé qui sera stocké dans la base de données. Cette technique offre de bonnes performances. Cependant, il est toujours vulnérable contre certaines attaques comme les attaques par dictionnaire.

En second lieu, les techniques qui changent le positionnement des minuties pour générer un nouvel ensemble sécurisé de points d'intérêts [Ratha *et al.* 2007, Yang *et al.* 2009, Ahmad *et al.* 2011]. [Ratha *et al.* 2007] ont proposé une solution intéressante qui appartient à cette catégorie. L'idée principale est d'appliquer des transformations géométriques sur la représentation des minuties. Trois types de transformation ont été testés : cartésienne, radiale et fonctionnelle. Cette solution offre une grande sécurité, car il est difficile de récupérer la représentation de minuties originale à partir du modèle transformé. Cependant, ces transformations augmentent le taux des variations intra-sujets dans la représentation sécurisé, ce qui dégrade considérablement la performance.

Enfin, les techniques qui génèrent une nouvelle représentation à partir de la représentation par minuties. Par exemple, [Ferrara *et al.* 2012] ont proposé une version protégée de *Minutia Cylinder-Code* (MCC) [Cappelli *et al.* 2010], qui est une nouvelle représentation

pour les empreintes digitales. MCC utilise, pour chaque minutie, un cylindre (un descripteur local) pour encoder l'information, spatiale (localisation) et directionnelle (orientation) entre la minutie et son voisinage, et créer le modèle de l'impression. Une transformation non inversible basée sur la projection de *Kullback-Leibler* [Goutis & Robert 1998] suivie d'une étape de binarisation ont été appliquées sur la MCC. Cette approche a démontré une très bonne performance, même si elle n'arrive pas à équilibrer efficacement la performance / précision avec la sécurité / confidentialité. Notre travail présenté dans cette thèse est principalement concerné et lié à ce genre de solutions.

5.3.4 Fingerprint Shell

L'idée principale de Fingerprint Shell est de construire des courbes spirales spéciales en utilisant les informations fournies par les minuties. Ces courbes sont stockées dans la base de données du système pour les utiliser directement dans la tâche de classification. Cette nouvelle représentation des empreintes digitales offre : la révocabilité, la diversité, la sécurité et la performance. Les étapes principales de Fingerprint Shell sont les suivantes :

Lors de l'enrôlement, pour chaque impression nous effectuons ces démarches :

- Extraction des minuties et les points singuliers [2] (Core et Delta).
- Calculer la distance entre chaque minutie et tous les points singuliers (c'est-à-dire pour chaque impression d'empreinte digitale, le nombre de courbes sera égal au nombre de points singuliers). Les distances entre les minuties et un point singulier sont invariantes avec les translations et les rotations. Malgré la présence de ces variations intra-sujet, ces distance ne changent pas d'une manière drastique, d'où l'idée de les utiliser au lieu des coordonnées / orientations des minuties utilisées dans les représentations traditionnelles.

2. Points singuliers (Figure 5.28) sont des régions spéciales dans une impression d'empreintes digitales où les crêtes sont caractérisées par une courbure très forte (c'est-à-dire, l'orientation et la fréquence locale peuvent se changer très rapidement près de ces points singulier). Ces points peuvent être classés en deux catégories : Core et Delta. Le nombre de points singuliers dans un modèle d'empreinte digitale est habituellement compris entre un et quatre points. En littérature, ces points ne sont pas considérés comme des minuties. Pour plus de détails vous pouvez consulter [Maltoni *et al.* 2003, Maltoni *et al.* 2009].

- Construction de Fingerprint Shell / Curve : nous trions les distances extraites dans un ordre croissant. Les distances triées sont utilisées pour construire plusieurs triangles rectangles contigus. Plus précisément, ces distances sont les hypoténuses des triangles rectangles (voir Figure 5.29). Nous conservons seulement la courbe spirale qui présente le modèle protégé de cette approche.

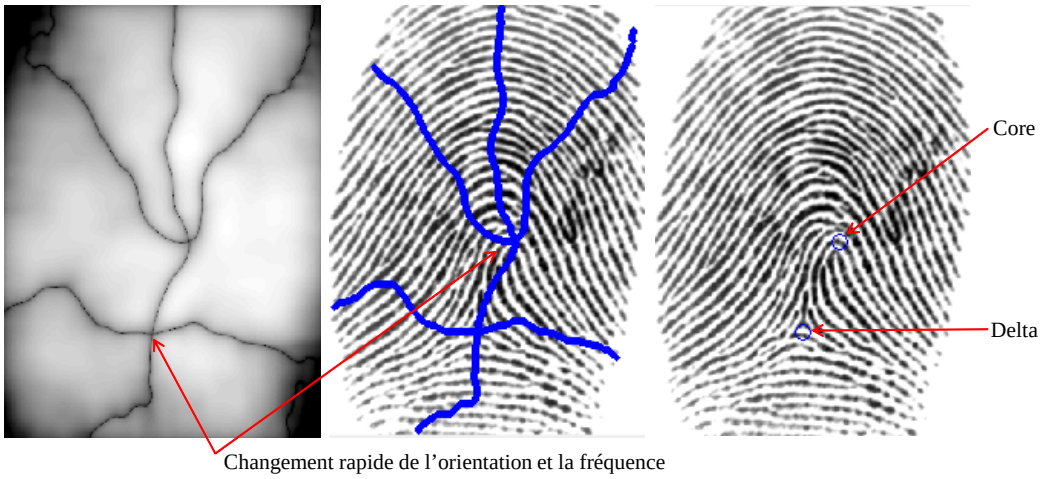


FIGURE 5.28 – Exemple de deux points singuliers.

Il convient de noter que pour le premier triangle, nous choisissons au hasard une distance initiale d_0 (voir Figure 5.29(a) et Algorithme 1 dans annexe A.5), pour l'autre côté de l'angle (première Cathète), la Cathète opposée est calculée en utilisant le théorème de Pythagore. En outre, d_0 est ajoutée à chaque distance extraite, avant le processus de construction des triangles, pour être en mesure de lancer notre algorithme, même dans le scénario où d_0 est supérieure à quelques distances extraites. Chaque utilisateur aura sa propre d_0 qui peut être considérée comme la clé de l'utilisateur (nous pouvons considérer d_0 comme une *clé utilisateur*). En pratique, cette stratégie réduit considérablement les fausses acceptations et augmente par conséquent la performance (voir notre expérimentation 5.3.5).

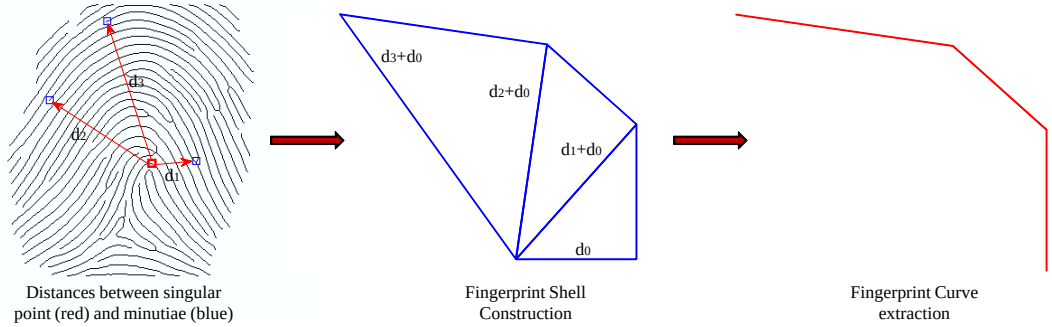
Lors de l'authentification, pour chaque image de test, nous utilisons les mêmes démarches appliquées sur les impressions de la formation, sauf pour le choix du point singulier. Pour les modèles de test, seulement le point singulier le plus proche du centre de l'image de test est choisi pour calculer les distances.

Pour comparer des courbes de test et de référence, nous appliquons la *distance de Hausdorff*[3] qui est largement utilisée dans la vision par ordinateur pour mesurer la différence entre deux formes. Pour deux ensembles de points A et B, la distance de Hausdorff est définie comme suit :

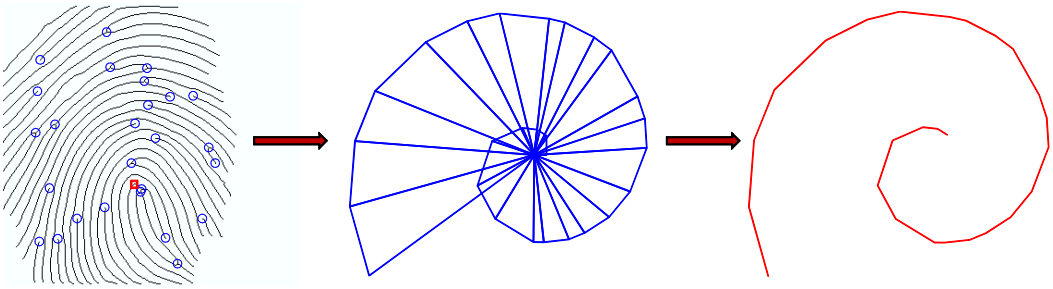
$$HD(A,B) = max(h(A,B), h(B,A)) \tag{5.4}$$

$$\text{avec} \quad h(A,B) = \max_{a \in A} \min_{b \in B} \| a - b \|$$

– $\| . \|$ est une fonction de la distance (par exemple, la distance euclidienne).



(a) Exemple simple de la construction de Fingerprint Shell/Curve



(b) Fingerprint Shell/Curve d'une empreinte digitale réelle

FIGURE 5.29 – Procédure générale de la construction de Fingerprint Shell.

La technique proposée est conforme aux exigences de la révocabilité, la diversité et la sécurité. En pratique, nous pouvons protéger un modèle compromis en modifiant la distance d_0 (révocabilité) ; la nouvelle courbe construite ne va pas correspondre avec le modèle volé, ce qui garantit la diversité (voir la Figure 5.30). Pour la sécurité, il est très difficile de récupérer les minuties originales (qui vont être utilisées également pour récupérer l'impression originale) à partir d'une courbe Fingerprint Shell volée. Tout d'abord,

3. http ://en.wikipedia.org/wiki/Hausdorff_distance

on analyse le pire des cas où l'adversaire a un accès à une courbe et il connaît le processus pour récupérer les distances entre le point singulier et les minuties extraites. En pratique, le nombre de possibilités pour mettre chacune des minuties autour du point singulier, en utilisant les distances récupérées, est infini. Cependant, même si nous supposons que, pour chaque distance, il n'y a que 360 possibilités de positionnement, le nombre de combinaisons possibles est de 360^n (n est le nombre de minuties). Alors selon cette complexité des attaques à force brute, nous pouvons conclure que, même dans le pire des cas, la sécurité de notre système est suffisamment robuste pour ce genre d'attaques. La performance, la diversité et la sécurité seront analysées encore dans la sous-section suivante.

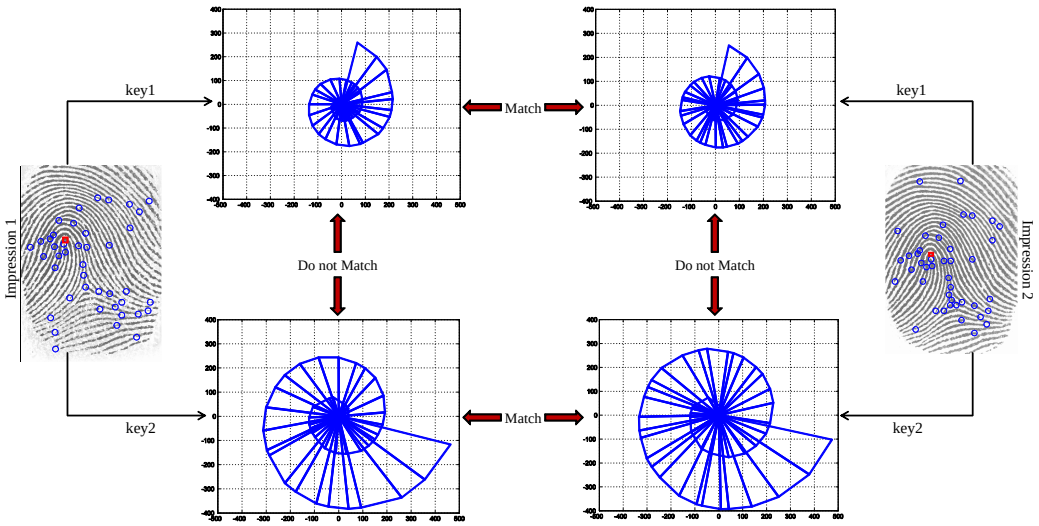


FIGURE 5.30 – Illustration de la révocabilité / diversité ; exemple de deux impressions de la même identité en utilisant deux différentes d_0.

5.3.5 Expérimentations et discussion

Dans cette section, nous évaluons la performance de la vérification de Fingerprint Shell en utilisant le protocole FVC (Fingerprint Verification Competition), présenté dans la section 4.2.1 du chapitre 4, et les bases de données FVC2002 DB1 et DB2 [Maio *et al.* 2002] d'empreintes digitales.

FVC2002 DB1 et DB2 contiennent 800 impressions, de diverse qualité, de 100 doigts

distincts (c'est-à-dire chaque personne est représentée par 8 impressions). La version d'essai du logiciel commercial VeriFinger SDK 6.0 [4] a été utilisée pour extraire les minuties.

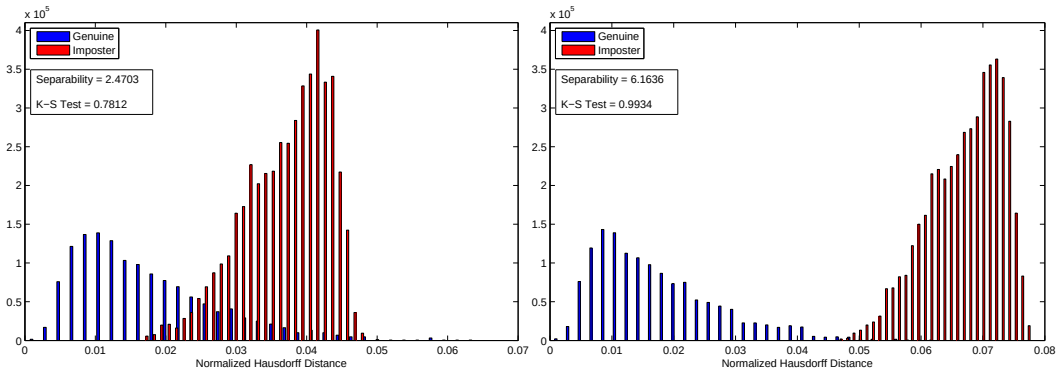
Les courbes de Fingerprint Shell sont construites comme décrit dans la section 5.3.4. Toutefois, pour utiliser correctement le protocole de vérification FVC et fournir une comparaison équitable avec les approches de l'état de l'art, on a utilisé seulement le point singulier le plus proche du centre de l'image pour calculer les distances. Il convient de noter que trois images dans FVC2002 DB1 et une image dans FVC2002 DB2 ne contiennent pas de points singuliers, ce qui signifie que le nombre de tentatives de reconnaissance possible en utilisant ces images rejetées, parmi les 2800 tentatives d'authentiques possibles, est 21 et 7 pour respectivement DB1 et DB2. Par conséquent, dans notre expérimentation, $REJ_{DB1} = 0.75\%$ et $REJ_{DB2} = 0.25\%$.

Tout d'abord, nous avons évalué l'importance d'utiliser un d_0 spécifique pour chaque utilisateur. Ainsi, nous avons calculé la séparabilité, le test de Kolmogorov-Smirnov et l'histogramme de distribution des scores légitime / imposteur, en utilisant la base de données FVC2002 ; pour montrer comment l'utilisation des d_0 spécifiques influence la discriminabilité. Dans le premier système, les gens s'inscrivent sans une clé utilisateur (c'est à dire, la même d_0 est utilisé pour tous les doigts). Dans le deuxième système, la clé utilisateur est requise (les clés sont choisies de façon aléatoire dans l'intervalle]0, 1.5555]). La Figure 5.31 illustre les résultats.

La Figure 5.31(a) montre la distribution des scores légitime / imposteur du premier système (sans clé utilisateur). Nous pouvons observer un certain chevauchement entre les deux distributions, ce qui explique les valeurs moyennes du test K-S (0,7812) et de séparabilité (2,4703). Ces valeurs sont augmentées considérablement (6,1636 et 0,9934 pour respectivement la séparabilité et le test K-S) en utilisant des clés utilisateur dans le deuxième système (Figure 5.31(b)), ce qui signifie que la discriminabilité est améliorée. Par conséquent, nous pouvons conclure que l'utilisation d'une d_0 spécifique pour chaque utilisateur réduit le taux de fausses acceptations, ce qui augmente la précision / performance.

Le but de notre deuxième expérimentation est d'évaluer la diversité de Fingerprint Shell

4. http ://www.neurotechnology.com



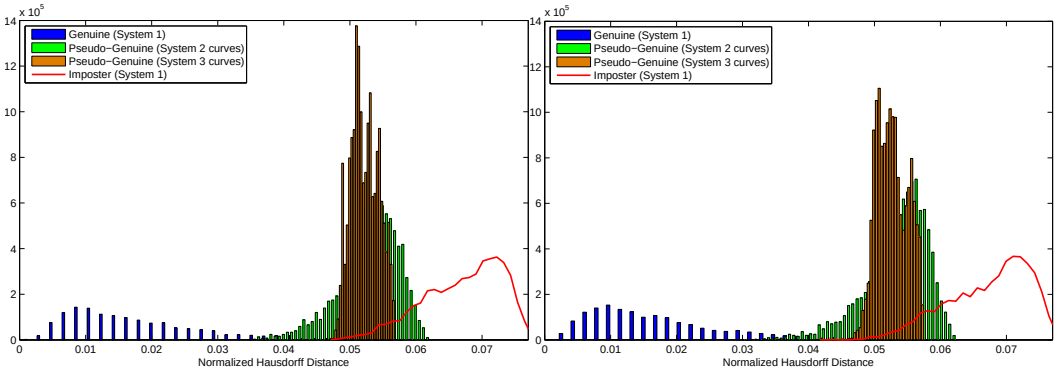
(a) Sans clé utilisateur (b) Avec clé utilisateur

FIGURE 5.31 – Histogramme de deux systèmes protégés par Fingerprint Shell en utilisant FVC2002 DB1.

(la résistance contre cross-matching). Il faut s'assurer que la courbe Fingerprint Shell d'un doigt ne permet pas la correspondance avec les courbes du même doigt dans d'autres systèmes protégés par la même technique. Pour chaque base de données, nous avons considéré trois systèmes qui s'inscrivent les mêmes doigts (identités) dans leurs bases de données. Les systèmes 1, 2 et 3 utilisent des clés qui sont choisies de façon aléatoire dans respectivement les intervalles]0, 1.5555], [100, 500] et [1000, 2000]. Pour chaque doigt dans le système 1, le même doigt dans les systèmes 2 et 3 est utilisé pour obtenir la *pseudo-légitime* distribution de la manière suivante : chaque courbe du système 1 est comparée avec toutes les courbes du même doigt dans les systèmes 2 et 3 (6400 tentatives pour chaque système si toutes les impressions sont inscrites avec succès ; 6355 tentatives pour DB1 et 6385 tentatives pour DB2 dans notre expérimentation). Les résultats sont illustrés sur la Figure 5.32.

La Figure 5.32 présente la distribution des scores légitime / imposteur du système 1 et les pseudo-légitimes distributions dans le même système en utilisant les courbes Fingerprint Shell du système 2 et 3. On peut observer que les deux pseudo-légitimes distributions sont bien séparées de la distribution des légitimes du système 1. En outre, ils sont plus proches de la distribution des imposteurs du système 1, ce qui signifie que le système 1 considère, la plupart du temps, les courbes Fingeprint Shell des systèmes 2 et 3 comme des imposteurs. Ainsi, nous pouvons conclure que la révocabilité et la diversité sont atteintes par notre approche proposée. Nous pouvons également remarquer que la pseudo-légitime

distribution du système 3 est plus séparée de la distribution des légitimes du système 1 que celle du système 2, ce qui signifie que la diversité, de deux systèmes basés sur l'approche Fingerprint Shell, augmente si les intervalles de clés sont bien séparées.



(a) FVC2002 DB1 (b) FVC2002 DB2

FIGURE 5.32 – Histogramme du système 1 et pseudo-légitimes distributions en utilisant les systèmes 2 et 3.

Le Tableau 5.5 fournit une comparaison de la précision de la vérification de Fingerprint Shell avec les approches de protection existantes qui utilisent le même protocole FVC. Il convient de noter que tous les algorithmes cités dans le Tableau 5.5 (à l'exception de [Boult *et al.* 2007]) sont des approches à un *seul facteur*. Cependant, Fingerprint Shell et [Boult *et al.* 2007] sont des techniques à *deux facteurs* qui combinent les informations fournies par une impression avec une clé secrète (pour Fingerprint Shell, les clés sont choisies ici de façon aléatoire dans l'intervalle]0, 100]). Nous pouvons observer que notre approche montre de bonnes performances en comparaison avec l'état de l'art.

TABLE 5.5 – Précision de vérification basée sur le protocole FVC (valeurs en %)

	FVC2002 DB1			FVC2002 DB2		
	ERR	FMR_{1000}	$Zero_{FMR}$	EER	FMR_{1000}	$Zero_{FMR}$
[Boult *et al.* 2007]	2.1	—	—	1.2	—	—
[Tulyakov *et al.* 2007]	3	—	—	—	—	—
[Ahn *et al.* 2008]	7.18	—	—	3.61	—	—
[Kumar *et al.* 2010]	—	—	—	4.98	—	—
[Ferrara *et al.* 2012]	1.88	3.14	5.07	0.99	1.43	2.54
Fingerprint Shell	2.03	4.18	6.36	1.01	1.39	2.21

Pour analyser la performance de Fingerprint Shell dans le scénario d'attaques à zéro effort, où l'adversaire connait d_0 et essaie de contourner le système en utilisant ses propres empreintes digitales, nous avons modifié le protocole d'évaluation FVC. Pour obtenir la distribution des scores imposteurs, la première courbe de chaque doigt est comparée avec la première courbe des doigts restants qui sont construits en utilisant la même d_0 de la courbe de référence (c'est-à-dire, 9900 attaques si toutes les premières impressions sont inscrites avec succès). Pour la distribution des scores légitimes, chaque impression est comparée avec les impressions restantes du même doigt (c'est-à-dire, 2800 tentatives si toutes les impressions sont inscrites avec succès). Il convient de noter que les clés sont choisies ici aléatoirement dans l'intervalle]0, 1000]. Les courbes ROC de Fingerprint Shell selon le scénario décrit sont illustrées sur la Figure 5.33.

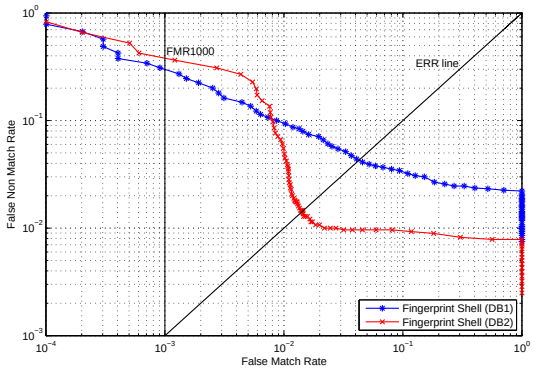


FIGURE 5.33 – Courbes ROC dans le scénario d'attaque à zéro effort en utilisant FVC2002 DB1 et DB2.

En général, nous pouvons observer que l'approche proposée conserve la performance des systèmes protégés, ce qui signifie que Fingerprint Shell résiste contre les attaques à zéro effort, même dans le scénario où l'adversaire connaît la clé utilisateur. Cependant, nous pouvons observer dans le Tableau 5.6, qui présente les valeurs ERR, FMR1000 et ZeroFMR calculées à partir de la Figure 5.33, que la performance est conservée seulement à proximité des points ERR (4,28% et 1,45% pour DB1 et DB2 respectivement). Fingerprint Shell perd la précision pour les seuils qui sont loin des points ERR (voir FMR_{1000} et Zero_{FMR} dans le Tableau 5.6). Par conséquent, nous pouvons conclure que, dans les applications de sécurité

basées sur la Fingerprint Shell, les systèmes doivent être exploités et utilisés seulement près du point ERR pour minimiser le succès des attaques à zéro effort.

TABLE 5.6 – Précision de la vérification de Fingerprint Shell dans le scénario d'attaque à zéro effort (valeurs en %)

	FVC2002 DB1			FVC2002 DB2		
	ERR	FMR_{1000}	$Zero_{FMR}$	EER	FMR_{1000}	$Zero_{FMR}$
Fingerprint Shell	4.28	27.14	94.00	1.45	36.46	99.04

5.4 Résumé du chapitre et conclusions

Dans ce chapitre, nous avons présenté deux nouvelles approches de la protection des modèles biométriques : Spiral Cube et Fingerprint Shell.

Spiral Cube est une nouvelle approche de la protection des modèles biométriques, qui sont sous forme de vecteurs, basée sur la projection aléatoire et le comportement chaotique de la suite logistique. Nous avons utilisé la suite logistique pour générer des vecteurs linéairement indépendants pour réaliser la projection aléatoire. Ces vecteurs sont stockés dans un cube spiral, qui est ensuite utilisé pour générer les matrices de protection. Notre mécanisme de sélection de vecteurs rend les matrices de projection dépendantes du modèle biométrique à protéger et de son identité. Notre approche fournit la révocabilité, la diversité et la sécurité, qui sont nécessaires dans une méthode idéale de protection. En outre, cette approche conserve et augmente les performances de reconnaissance (en raison de l'utilisation d'une matrice de projection dynamique pour chaque identité). Ainsi, elle gère mieux les variations intra-sujets. Nos résultats expérimentaux indiquent que la conception des systèmes non protégés influence relativement l'efficacité des régimes de protection. Aussi, nos résultats confirment que la présence de variations intra-sujets font des approches de transformation non inversibles moins résistant aux attaques possibles, ce qui nécessite beaucoup moins de tentatives pour compromettre la sécurité.

Fingerprint Shell est une nouvelle approche de protection des empreintes digitales. Les informations fournies par les minuties sont utilisées pour construire une nouvelle repré-

sentation basée sur des courbes spirales spéciales, qui est utilisée dans la tâche de reconnaissance au lieu de la représentation traditionnelle basée sur les minuties. Notre approche fournit la révocabilité, la diversité et la sécurité. En outre, nos résultats expérimentaux indiquent que cette technique préserve la performance de reconnaissance. La performance / précision de Fingerprint Shell sont liées à deux facteurs essentiels : d'une part, la précision de l'extraction des minuties et d'autre part, la présence et la précision de la détection des points singuliers. Cependant, contrairement aux plusieurs systèmes de protection des empreintes digitales, la performance de Fingerprint Shell est moins sensible à la translation / rotation des impressions.

CHAPITRE 6

Conclusion générale et perspective

Cette thèse a examiné le problème de la protection des systèmes de sécurité biométriques. Bien que les systèmes de sécurité biométriques aient des avantages inhérents par rapport aux systèmes traditionnels d'authentification personnelle, le problème d'assurer la sécurité et la confidentialité des données biométriques demeure critique. L'utilisation croissante de la biométrie dans les applications de la sécurité a suscité un regain d'intérêt pour la recherche et l'exploration de nouvelles méthodes pour attaquer les systèmes biométriques. Ces recherches ont prouvé que ces systèmes sont vulnérables à un certain nombre d'attaques. Notre principal objectif a été l'évaluation des menaces liées aux attaques contre les modèles biométriques et le développement des schémas de protection génériques pour ces modèles afin d'améliorer la robustesse générale des systèmes biométriques.

Le but du chapitre 1 a été d'introduire le problème de la sécurité dans les systèmes biométriques, et de clarifier le contexte de ce travail, la perspective suivie lors de l'élaboration de la thèse, les objectifs et les contributions principales. Le chapitre 2 a été consacré à introduire les menaces générales contre les applications de sécurité, détailler les vulnérabilités des systèmes biométriques ; et aborder les exigences d'un schéma idéal de protection des modèles biométriques. Dans le chapitre 3, nous avons présenté un état de l'art des travaux sur la protection des systèmes de sécurité biométriques en mettant l'accent sur les méthodes de la protection des modèles biométriques. Le chapitre 4 a abordé les différentes méthodologies statistiques disponibles pour évaluer la performance / sécurité des systèmes biométriques / schémas de protection. Dans le Chapitre 5, nous avons présenté nos propres approches pour la protection des modèles biométriques : Spiral Cube et Fingerprint Shell. Nos séries d'expériences dans ce chapitre ont prouvé que la conception des systèmes non

protégés influence relativement l'efficacité des régimes de protection et que la présence de variations intra-sujets rend des approches de protection moins résistantes aux attaques possibles (malgré que la performance est conservée).

Nous voulons bien confirmer à la fin de cette thèse, comme nous l'avons confirmé à l'introduction, que la sécurité absolue n'existe pas. Il est vraiment très important de comprendre, tout simplement, que les systèmes de reconnaissance personnelle (traditionnels et biométriques) parfaits n'existent pas ; et peut-être ils n'existeront jamais. Cependant, Nous pouvons dire que les systèmes d'authentification basés sur la biométrie peuvent toujours fournir l'*assurance de l'identité* [1], qui est fondamentale pour la sécurité des systèmes, si on l'utilise avec prudence et en collaboration avec d'autres techniques de protection (cryptographie, signature numérique, horodatage, challenge-réponse, etc.).

Ce travail peut être considéré comme une base pour les travaux futurs dans cette direction de recherche. Les travaux futurs sont suggérés vers l'optimisation des approches Spiral Cube et Fingerprint Shell. Nous envisageons de tester Spiral Cube sur des grandes bases de données. En outre, nous envisageons de résoudre le problème de la génération des matrices de projection en utilisant l'orthogonalisation Gram-Schmidt qui prend du temps. Il existe des méthodes moins coûteuses qui ne nécessitent pas l'application d'une orthogonalisation telle que [Achlioptas 2003]. Le test de cet algorithme est un de nos objectifs de travaux futurs. Pour Fingerprint Shell, nous allons la tester en utilisant des bases de données plus grandes qui sont caractérisées par la présence de variations intra-sujets importantes. Aussi, nous comptons améliorer Fingerprint Shell en utilisant d'autres caractéristiques des empreintes digitales (par exemple, le texture) pour construire les courbes. En outre, nos plans futurs incluent la conception de nouveaux systèmes de protection pour les systèmes multimodaux et l'inclusion des techniques de tatouage dans nos schémas de protection.

1. http ://en.wikipedia.org/wiki/Identity_assurance

CHAPITRE 7

Résumé étendu en arabe

باعتباراللغة العربية هي اللغة الرسمية الأولى للمملكة المغربية، و إيماناً منا بضرورة تعزيز وجودها في مختلف المجالات العلمية الحديثة، نقدم في هذا الفصل ملخصاً مُطولاً للإشكاليات التي تعالجها هذه الأطروحة كمساهمة جد متواضعة في خضم كل المجهودات المبذولة منذ عدة سنوات من أجل تعريب واستخدام اللغة العربية في مجال علوم و هندسة الحاسوب.

تم إنجاز هذه الأطروحة في الفترة الممتدة بين ديسمبر ٢٠١٠ و يونيو ٢٠١٤ تحت إدارة الأساتذة محمد رْزِيزا (كلية العلوم، جامعة محمد الخامس ـ أكدال، المغرب) و جورج بِبِس (جامعة نيفادا ـ رينو، الولايات المتحدة الأمريكية)، و إشراف الأساتذة سناء غزالي (جامعة الملك سعود ـ الرياض، السعودية) و مونية مكرام (مدرسة علوم الإعلام ـ الرباط، المغرب). تخلل إنجاز هذا العمل القيام بعدة زيارات ل 'مختبر الرؤية الحاسوبية' Computer Vision Laboratory بجامعة نيفادا ـ رينو بدعم و تمويل من اللجنة المغربية الأمريكية للتبادل التربوي و الثقافي MACECE.

فيما يلي، نقدم بإيجاز الخطوط العريضة للإشكاليات و المقاربات التي تم طرحها في هذا التقرير، و التي تم أيضاً تقديم و نشر نتائجها في العديد من المؤتمرات و الصحف العلمية الذائعة الصيت في مجال التعرف على الأنماط، و علوم و هندسة الحاسوب عموماً:

حماية الأنظمة الأمنية البيومترية: مساهمات في حماية النماذج البيومترية

شعيب مجاهدي

مع النمو الهائل الذي تعرفه تقنيات التواصل و الاتصال عن بعد، سواء من حيث الحجم أوالتنوع (المعاملات المالية، حركة المسافرين، الحصول على الخدمات، الخ)، برزت عدة مخاوف و توصيات دولية تلح على ضرورة التصدي لعدة مشاكل مُرتبطة أساساً بالجريمة الإلكترونية، الإحتيال، الإرهاب و سرقة الهوية. يمكننا تعريف سرقة الهوية بالإستخدام غير الشرعي أو غير المصرح به لمعلومات شخصية مسروقة (كلمة سر، بطاقة هوية، بصمات الأصابع، الخ.) للإستفادة من خدمة أو لتخريبها، أو للقيام بمزيج من هذه الأنواع من الانتهاكات. على سبيل المثال، في أحدث تقرير لوزارة العدل الأميركية، يُقدر عدد ضحايا سرقة الهوية في الولايات المتحدة كل سنة ب ١١ ٥٧١ ٩٠٠ و تُقدر الخسارة المالية الإجمالية التي تُعزَى إلى هذه المشكلة في عام ٢٠١٣ ب ٢١ مليار دولار (بعدما كانت ١٣.٢ مليار دولار في عام ٢٠١٠). هذا يعطي صورة واضحة عن التهديدات الكبيرة التي يطرحها مشكل سرقة الهوية على عدة مستويات.

أمام هذه المسؤوليات السياسية \ الإقتصاية من ناحية، والحاجة الملحة إلى توفير الحماية اللازمة للحياة الخاصة لأفراد المجتمع من ناحية أخرى، أصبحت تثير أنظمة التحقق من الهوية اهتماماً متزايداً و اقتحمت مجالات مختلفة، مثل المصارف، المرافق العمومية و قطاع النقل، الخ. تسعى جميع أنواع أنظمة التحقق من الهوية إلى توفير وسيلة موثوقة، بسيطة وعملية، للتحقق من هوية الشخص تلقائياً، دون مساعدة من شخص آخر. يتوجب على هذه الأنظمة تحديد الأشخاص بدقة، بسرعة، بفعالية، بأقل تكلفة، دون انتهاك لخصوصية المستخدمين، ودون تغييرات جذرية في البنيات التحتية الموجودة.

تُعتبَر أنظمة التحقق من الهوية التقليدية، التي تستخدم كلمات السر أو بطاقات الهوية، غير قادرة على تلبية كل هذه المتطلبات بفعالية. على سبيل المثال لا الحصر، يَستخدم معظم الأشخاص كلمات سر، مُكونَةً من الحروف و \ أو الأرقام، التي يمكن تذكُرها بسهولة كالأسماء، وأعياد الميلاد والشخصيات المشهورة أو الموسيقى المفضلة. غير أنه في الواقع التطبيقي المُحترِف، يجعل هذا السلوكُ كلمات السر سهلة التخمين باستخدام هجوم القوة العمياء (Brute-force attack) أو هجوم القاموس (Dictionary attack). إضافة إلى ذلك، على الرغم من أنه من المستحسن استخدام كلمات مرور مختلفة لكل خدمة على حدة، يستخدم معظم الأشخاص نفس كلمة السر في جميع الخدمات. إذا تم الإستحواذ على كلمة مرور واحدة فقط، سوف تكون كافة التطبيقات مُهددَة إن لم نقل مكشوفة. في الممارسة العملية، تُعتبَر كلمات السر العشوائية والطويلة أكثر أمناً، لكنها في المقابل أكثر صعوبة للتذكر، مما يدفع ببعض المستخدمين إلى كتابتها في مُسَوداتهم أو في ملفات رقمية غير آمنة.

في المقابل، أثبت أنظمة التحقق من الهوية البيومترية التي تستخدم الخصائص الفيزيولوجية (الوجه وبصمات الأصابع، الخ.) والسلوكية (التوقيع، والصوت، الخ.) أولويةً وكفاءةً بالمقارنة مع الأنظمة التقليدية. لا تعتمد عموماً الأنظمة البيومترية على ما لدى الشخص أو ما يعرف؛ و الغرض الأساسي من تصميمها هو محاكاة نظام التعرف البشري من قبل جهاز الحاسوب لأستخدامه في بعض الخدمات مثل بطاقة الهوية الوطنية، رخصة السائق، الضمان الاجتماعي، مراقبة الحدود، مراقبة الجوازات، الرصد عن بعد، الدخول إلى المواقع الإلكترونية، تأمين المباني، العلوم الاستعرافية، التحقيق الجنائي والإرهاب، الخ.

تتميز مختلف الأنظمة البيومترية عن الأنظمة التقليدية بكونها تستخدم خصائصاً حيويةً كونية، فريدة من نوعها، دائمة، و موثوقة بشكل أكبر، لأن المعلومات البيومترية لا يمكن أن تَضيع، أن تُخمَن بسهولة، أو أن تُنسَى (تُفيد بعض التقارير إلى أن ما يقرب من ٢٥٪ المكالمات الوافدة إلى مركز اتصال الأنظمة التقليدية يكون موضوعها هو نسيان كلمات السر). لكن، رغم أن الأنظمة البيومترية قادرة على زيادة السلامة في العديد من الأنظمة الأمنية، فإنها، مثل أي نظام أمني آخر، تعاني من ثغرات ونقاطِ ضعف.

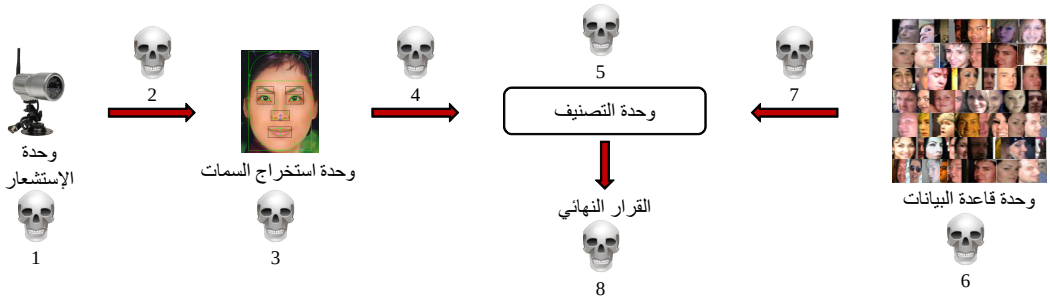
لقد أدى تزايد استخدام القياسات الحيوية في تصميم الأنظمة الأمنية إلى تنامي الإهتمام بتمويل دراسات للبحث والتنقيب عن أساليب جديدة لمهاجمة أنظمة التحقق من الهوية البيومترية. حيث أظهرت هذه الدراسات أن استخدام القياسات الحيوية قد أدى إلى انبثاق مشاكل و تحديات جديدة متعلقة أساساً بسلامة وحماية البيانات الشخصية للمستخدمين. مشاكل و تحديات أكثر تعقيداً من تلك التي تطرحها الأنظمة التقليدية. يمكننا تلخيصها بإيجاز على النحو التالي [Ratha et al. 2006]:

- القياسات الحيوية غير سرية: رغم أن الخصائص البيومترية فريدة من نوعها لدى كل فرد، إلا أنها لا تُوفر السرية. في الواقع التطبيقي، تَستخدِم الأنظمة البيومترية عدة أنواع من الخصائص البيومترية (الوجه، قزحية العين، بصمات الأصابع، التوقيع، الصوت، الخ.) التي يمكن تقليدها أو أخذها دون وعي أو موافقة مالِكها الشرعي. على سبيل المثال، يملك كل شخص أشكال بصمات للأصابع خاصة به (التفرد)، ولكن في المقابل يترك هذا الشخص أثراً لبصماته في أغلب الأماكن التي يلمسها (انعدام السرية). في هذا السياق، يمكن القول أن المعلومات البيومترية ليست سرية. ما يجعل مشكلة ضمان أمن وخصوصية البيانات البيومترية حرجة للغاية.
- القياسات الحيوية غير قابلة للإلغاء: يتم تسجيل كل فرد في النظام البيومتري بواسطة نموذج للخصائص. إذا سرق هذا النموذج، سيواجه النظام تهديدات أمنية خطيرة، لأنه، على عكس كلمة سر أو بطاقة هوية مسروقة، ليس من الممكن لمستخدم شرعي أن يُلغي نماذجه البيومترية المسروقة ويَستبدلها بمجموعة أخرى من الخصائص. مما قد يمنع أيضا المستخدِم من إعادة تسجيل نفسه من جديد في النظام.
- للقياسات الحيوية استخداماتٌ ثانوية: صُمِمَت الأنظمة البيومترية خِصيصا للتطبيقات الأمنية، ولكن يمكن استخدامها بشكل مختلف للغاية في إطارات و اعتبارات أخرى. على سبيل المثال، تم تصميم رخصة السياقة لإثبات الهوية وشرعية السياقة إلى ضابط الشرطة، ولكن يمكن أن تستخدم أيضاً لإثبات العمر، والإسم، وحتى المواطنة في سياقات موضوعية أخرى. جانب آخر من جوانب هذه المشكلة هو انتهاك الخصوصية. إذا كان الشخص يستخدم نفس الخاصية البيومترية في العديد من التطبيقات المختلفة، فيمكن اقتِفاءه بسهولة في حالات معينة، مما يشكل انتهاكاً خطيراً لخصوصيته.

لقد جعلت هذه الجملة من المشاكل أنظمةَ الأمن البيومترية تعاني من العديد من نقاط الضعف التي يمكن تقسيمها إلى فئتين رئيسيتين. أولا، نقاط ضعف بالنسبة للهجمات التي يمكن أن تُشَن ضد أي نظام أمني كيفما كان نوعه [Ferguson et al. 2010]. لقد جرت العادة على تثبيت الأنظمة البيومترية على خادم معلوماتي، مما يجعلها عرضة لجميع أنواع الهجمات التي تهدد أنظمة الكمبيوتر الحديثة مثل الفيروسات الحاسوبية والبرامج الخبيثة. ثانياً، نقاط ضعف بالنسبة لهجمات تم تصميمُها خصيصاً لتُشن ضد أنظمة تحديد الهوية البيومترية، والتي يمكن أيضا تقسيمها إلى فئتين: الهجمات بمجهود منعدم (Zero effort attack) والفشل بسبب هجوم مُعادِي (Adversary attack).

يُمكن تعريف الهجوم منعدم المجهود بتدهور كفاءة و أمن النظام بسبب اتخاده لقرار خاطئ أثناء التحقق من هوية ما. يرتكب عادةً نظام التحقق من الهوية نوعين من الأخطاء أثناء عملية اتخاد القرار: الرفض الخاطئ، الذي تُسببه عادةً التغيرات في خصائص الشخص نفسه (التي تُعزَى إلى عدة عوامل حسب طبيعة الخاصية البيومترية المُستعمَلة كتعبيرات الوجه و ظروف الإضاءة على سبيل المثال بالنسبة لأنظمة التحقق من الوجه)، و القبول الخاطئ الذي يسببه عادةً التشابه البدني بين الأفراد أو تخفيض العتبة الأمنية (Threshold) للنظام بهدف رفع كفاءته.

بالنسبة للهجوم المُعادِي. يَستغِل عموماً الأعداء بِنْيَة أنظمة التحقق من الهوية (شكل ١) لشن هجمات محددة على واحد أو أكثر من الوحدات و \ أو القنوات. تتكون جميع الأنظمة البيومترية من أربع وحدات رئيسية تتواصل فيما بينها باستخدام عدة قنوات: وحدة الإستشعار التي يتم استخدامها لاتقاط و إدخال البيانات البيومترية للمستخدم (يتم ذلك باستخدام الأداة المناسبة حسب الخاصية البيومترية، كاميرا، ميكرفون، إلخ.). وحدة استخراج السمات التي تقوم بتحديد الميزات الأكثر أهمية في صورة بعثت بها وحدة الإستشعار لبناء نموذج اختبار بيومتري. وحدة قاعدة البيانات التي تحتوي على النماذج البيومترية للمستخدمين الشرعيين للنظام (سبق تسجيلهم قبل مرحلة الإستخدام). و أخيراً وحدة التصنيف التي تعد مسؤولة عن مقارنة نماذج الإختبار البيومتري مع النماذج المُخزنة في وحدة قاعدة البيانات لاتخاذ القرار النهائي للنظام. فتحت هذه البِنْيَة المجال لشن عدة أنواع من الهجمات الخاصة على الأنظمة البيومترية.



شكل ١ : نقاط و مستويات الهجوم على نظام بيومتري.

لقد تم تقديم هذه الهجمات في عدة أشكال مختلفة، باسخدام عدة أساليب ومن خلال عدة وجهات نظر [Ratha et al. 2001, Ratha et al. 2003, Adler 2005, Jain et al. 2006, Roberts 2007, Jain et al. 2008]. نقدم في هذا لتقرير النموذج المُقترَح في [Ratha et al. 2001]. حددت هذه الدراسة ثماني نقاط أو مستويات للهجوم في بنية نظام التحقق من الهوية البيومتري (شكل ١). يمكننا تلخيصها كما يلي:

(١). يعتمد الهجوم في هذا المستوى على تقديم بيانات بيومترية مُزوَرة أو مُقلَدة إلى وحدة الإستشعار (قزحية أو بصمة مُزورَة، قناع، توقيع مُقلَد، تسجيل صوتي، الخ).

(٢). في هذا المستوى، يتم التجسس على قناة التواصل بين وحدة الإستشعار و وحدة استخراج السمات لسرقة صورة للخاصيات البيومترية لمستخدم شرعي. يتم استخدام هذه الصورة لاحقاً في نفس القناة لاختراق النظام.

(٣). في هذا المستوى، يتم استبدال وحدة استخراج السمات ببرنامج حصان طروادة (Trojan Horse) الذي يعمل وفق مواصفات احتالية تخدم رغبات مُصمِمه.

(٤). يتم التجسس في هذا المستوى على قناة التواصل بين وحدة استخراج السمات و وحدة التصنيف لسرقة نموذج بيومتري لمستخدم شرعي يتم استخدامه لاحقاً لاختراق النظام.

(٥). يُستخدَم في هذا المستوى برنامجٌ من نوع حصان طروادة ليَتقمص دور المُصنِف لتقديم مجموع تطابق (Matching score) يُخوِل الدخول غير الشرعي لمصمم حصان طروادة، مُلغِياً بذلك لدور وحدة التصنيف الحقيقية.

(٦). يُشَن عادةً الهجوم في هذا المستوى ضد النماذج البيومترية المُخزَنة في وحدة قاعدة البيانات (سرقة، استبدال، حذف، تعديل النماذج). يمكن شن هذا الهجوم أثناء مرحلة التسجيل في النظام، خلال مرحلة التحقق، أو في أي وقت آخر مباشرةً ضد وحدة قاعدة البيانات. تجدر الإشارة إلى أنه في الأنظمة البيومترية التي تَستخدم البطاقات الذكية (Smart card)، يتم تخزين النماذج في بطاقات المستخدمين؛ في حالة فقدان البطاقة أو سرقتها، وإذا لم تكن مَحمِيةً بشكل كاف، يمكن استخراج النماذج البيومترية المُخزَنة بسهولة.

(٧). في هذا المستوى، يتم اعتراض سبيل النماذج البيومترية في قناة التواصل بين وحدة قاعدة البيانات و وحدة التصنيف، ليُعادَ استخدامها لاحقاً على نفس القناة.

(٨). يُمْكن التجسس على القناة بين وحدة التصنيف والتطبيق الذي أرسل طلب التحقق من الهوية للاستحواذ على إجابة المُصنِف وحِفْظها. هذه المعلومة يُمْكن إعادة استخدامها لاحقاً في نفس القناة.

يَعتمد كل هجوم من هذه الهجمات على سلسلة من الموارد والاحتياجات الخاصة، الأمر الذي يجعل صعوبة تصميم كل هجوم على حدة، شدتَه و كذا خطورتَه تختلف جهرياً. يُمْكن اعتبار الهجوم في المستوى ٦، ضد النماذج البيومترية المخزنة في وحدة قاعدة البيانات، مصدر قلق كبير للباحثين في مجال الأمن المعلوماتي و واحدة من الهجمات الأكثر تدميراً ضد أنظمة التحقق من الهوية البيومترية؛ من ناحية أولى لوجود علاقة قوية بين النماذج البيومترية وهوية مالكها، و من ناحية ثانية لطبيعة النماذج البيومترية الغير قابلة للنقض و الإلغاء. علاوة على ذلك، يرتبط هذا الهجوم بطريقة أو بأخرى بجميع الهجمات الأخرى في باقي المستويات. كما أن استخدام تقنيات التشفير الكلاسيكية (AES, RSA, etc.) لحماية النماذج البيومترية غير مناسب لعدة أسباب: أولاً، يستحيل إجراء المقارنات في مجال التشفير، لأن التشفير هو عموماً دالةٌ رياضية غير سلِسة، مما يؤدي إلى خلق اختلافات كبيرة جدا ين النماذج المُشفَرة مهما كانت الاختلافات جد صغيرة بين النماذج المُستخرَجة من البيانات البيومترية الخام (و هو الحال دائما في الممارسة التطبيقية). ثانياً، القيام بفك تشفير النماذج البيومترية أثناء كل محاولة للتحقق من الهوية يجعلها عُرْضَة لهجوم التنصت. ثالثاً، يَعتمد أمن هذه الأنظمة اعتماداً كلياً على أمن مفتاح التشفير.

نعتقد، مثل العديد من الدراسات الأخرى والتوصيات في هذا المجال [ISO/IEC 2011]، أن دراسة و تقييم التهديدات المُتصِلة بالهجوم في المستوى ٦ و كذا تطوير خطط و تقنيات فعالة لحماية النماذج البيومترية، هو الطريق الصحيح لتطوير تقنية بيومترية أكثر قوة و أكثر أمنا. هذا هو المنظور و التصور المُتبَع في هذه الأطروحة.

باختصار، هناك أربعة أسباب أساسية تجعل من حماية النماذج البيومترية تحديا رئيسياً، يؤدي حله إلى تحسين أمن أنظمة التحقق من الهوية البومترية بفعالية:

(١). مشكلة عدم القدرة على إلغاء النماذج البيومترية. من المعروف أنه في حالة الأنظمة التقليدية، إذا ما تم سرقة كلمة السر، فمن السهل إنشاء كلمة سر جديدة وإزالة الكلمة المسروقة من قاعدة البيانات و إضافتها إلى قائمة النقض أو الإلغاء. على النقيض من ذلك، إذا تم سرقة نموذج بيومتري، لا يمكن تغييره (السمة البيومترية وحيدة و فريدة من نوعها). لذا صار مطلوباً بإلحاح تطوير تقنيات حماية تُوفِر إمكانية إلغاء النماذج المسروقة.

(٢). مشكلة إعادة بناء الصور الأصلية باستخدام نماذج بيومترية مسروقة. صحيح أنه، على عكس كلمة سر مسروقة، ليس من السهولة بما كان استخدام نموذج بيومتري مسروق بشكل صحيح من قِبَل خصم غير مُتخصِص، ولكنه لا ينبغي أن نَفترِض دائماً أن الخصوم سيظلون غير ماهرين و غير متخصصين. يجب على تقنيات حماية النماذج البيومترية ضمان أن الخصم لا يمكنه استرداد المعلومات الأصلية من خلال نماذج مسروقة.

(٣). مشكلة استخدام نفس السمة البيومترية في عدة أنظمة أمنية بيومترية في آن واحد. إذا تم تسجيل مستخدم في العديد من الأنظمة التي تستخدم نفس الخاصية البيومترية، و سُرِق أحد نماذجه من أحد هذه الأنظمة؛ ستصير كل هذه الأنظمة مُهدَدة ويمكن أيضاً تَتَبع هذا المستخدم في كل مكان. بعبارة أخرى، إن عدم وجود التنوع بين نماذج مُستخرَجة من نفس السمة البيومترية يُهدِد بشدة أمن وخصوصية مُستعمِلي الأنظمة البيومترية.

(٤). مشكلة الصلة القوية بين سرقة النماذج البيومترية وشن باقي الهجمات المحتملة ضد أنظمة التحقق من الهوية البيومترية. في معظم الأحيان، للقيام بشن هجوم ضد نظام التحقق من الهوية، هناك حاجة إلى الحصول على نموذج مسروق. لذا ينبغي أن لا تكون النماذج المحمية (المسروقة) مفيدةً لشن أنواع أخرى من هجمات.

تُجْمِع العديد من الدراسات على أن تقنية حماية النماذج البيومترية المثالية يجب أن تستوفي الشروط التالية [Jain et al. 2008, Breebaart et al. 2009, Campisi 2013]:

(١). التنوع: لا ينبغي على النماذج البيومترية المحمية (و التي تنتمي إلى نفس الهوية و المُسجَلة في العديد من الأنظمة البيومترية) أن تتوافق مع بعضها البعض لتجنب تتبع الشخص في مُختلَف التطبيقات وضمان خصوصيته. بعبارة أخرى، ينبغي أن يكون من الممكن بناء عدد كبير من النماذج المحمية (التي لا تتطابق) من نفس النموذج الأصلي (غير المحمي) ليكون الشخص قادراً على استخدام نفس السمة البيومترية في عدة أنظمة مُختلِفة.

(٢). النقض: ينبغي أن يكون من الممكن إلغاء نموذج بيومتري مُنتهَك وإنشاء نموذج جديد يستند على نفس النموذج الأصلي (غير المحمي). النقض هو نتيجة مباشرة للتنوع. إذا كانت تُوفِر تقنية للحماية التنوع، سيكون من الممكن بناء نماذج محمية جديدة و استبدال النماذج القديمة المهددة أو المسروقة (التي سيتم تخزينها في قائمة النقض (Revocation list)).

(٣). الأمن: يجب أن يكون من الصعب، من وجهة نظر حسابية، استعادة النموذج الأصلي من خلال نموذج محمي. من النتائج الأساسية التي يفرضها هذا الشرط هو أن عملية التصنيف يجب أن تتم في فضاء أو مجال النماذج المحمية، مما قد يؤدي إلى تدهور ملحوظ في كفاءة النظام. تجدر الإشارة إلى أن هذا الشرط (الأمن) يختلف عن مفهوم الأمن الشامل للنظام البيومتري الذي هو نتيجةٌ لتوفير جميع أساليب الحماية الممكنة في نظام التحقق من الهوية البيومتري (كتشفير البيانات في القنوات، الخ) لتجنب كل التهديدات المحتملة في جميع مستويات الهجوم التي سبق تقديمها (الشكل ١).

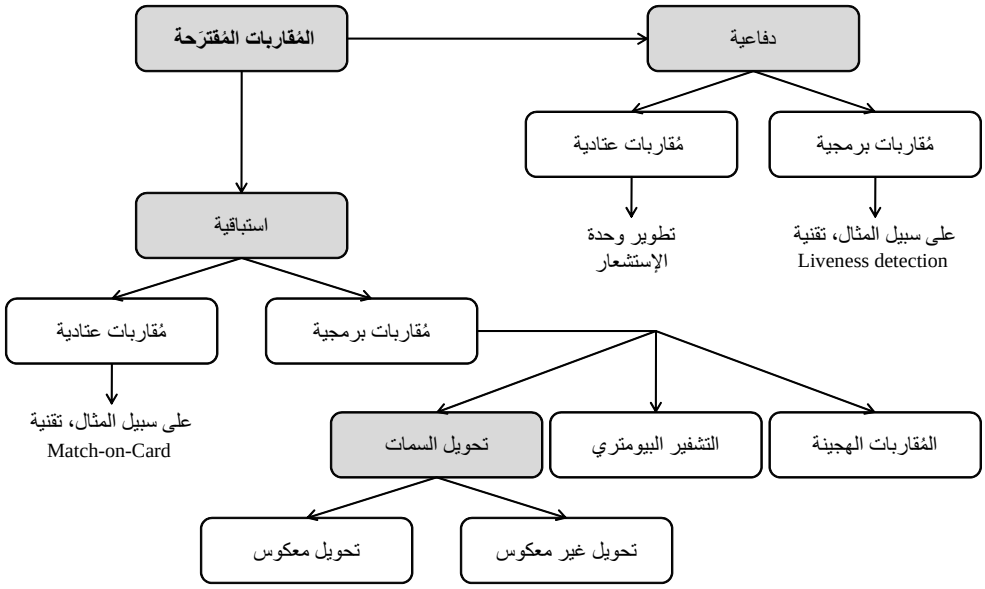
(٤). الكفاءة: لا يجب أن تقوم تقنية حماية النماذج البيومترية بإضعاف كفاءة التعرف، بشكل كبير، مقارنةً بالنظام البيومتري الأصلي (غير المحمي). إذا تدهورت الكفاءة بشكل كبير، يصير ممكناً شن هجوم المجهود المنعدم (Zero effort attack) بسهولة و بنِسَب نجاح أكبرَ مقارنةً بباقي الهجمات.

يجب على تقنيات الحماية المُقترحَة أن تُتحقِق هذه المُتطلَبات الأربعة في وقت واحد لحماية النماذج البيومترية بشكل فعال. يُشكِل تصميم تقنيات حماية النماذج البيومترية (التي تستجيب لجميع المتطلبات) تحديا صعبا للغاية بسبب ضرورة إدارة و ترويض التغيرات في خصائص الشخص (لأن التقاط عينات متعددة من نفس السمة البيومترية لا يؤدي إلى بناء مجموعة نماذج أصلية مُتماثَلة و قابلة للتطابق). مما يجعل تقنيات الحماية غير قادرة على توفير الأمن والكفاءة في وقت واحد. معظم هذه الحلول تضحي بالكفاءة لفائدة الأمن أو العكس. إضافةً إلى ذلك، يَعُوق تمثيل أو شكل النماذج البيومترية تصميم تقنيات حماية عامة وشاملة. يتم تخزين النماذج البيومترية في قاعدة بيانات معظم الأنظمة البيومترية على شكل مُتجهات (Vectors). بالمقابل، يتم تخزينها على شكل نقاط مُهمة (Interest points) في أنظمة أخرى (على سبيل المثال، التفصيلات (Minutiae) في أنظمة التعرف على بصمات الأصابع)، الأمر الذي يتطلب تصميم تقنيات حماية تُلائم كل شكل أو تمثيل على حدة. باختصار، لقد صار إشكال حماية النماذج البيومترية موضوع بحث نَشِط يجذب جهود بحث مكثفة نظراً لتطبيقاته المُحتمَلة في عدة مجالات وكذا التحدي الكبير الذي يطرحه.

في الماضي القريب، كانت تتمثل أهداف البحث في مجال القياسات الحيوية على تطوير الدقة والسرعة والتكلفة والكفاءة. لكنه في الآونة الأخيرة فقط، بدأت تتجه أنظار الباحثين نحو قضايا أمن وخصوصية أنظمة التحقق من الهوية البيومترية. لماذا يجب علينا أن نثق في التكنولوجيات البيومترية؟ كيف يمكننا تأمينها؟ مالذي يضمن مستوى الأمن التي توفره أنظمة التحقق من الهوية البومترية؟ ماذا لو سُرِقت بياناتي البيومترية؟ هذه الأسئلة وأخرى مماثلة أصبحت مُلِحة، و في حاجة إلى إجابات مقنعة.

للإجابة على هذه الأسئلة وحل هذه المشاكل، حاولت العديد من المبادرات الأكاديمية، التجارية و الحكومية، تطويرَ تقنيات جديدة لحماية أنظمة التحقق من الهوية البيومترية، بما في ذلك تقنيات حماية النماذج البيومترية. لكل من الحلول المُتاحة مزاياه و عيوبه الخاصة، و لا تزال عموماً غير ناضجة بما فيه الكفاية ليتم استعمالها على نطاق واسع؛ فهي لا تستجيب في نفس الوقت لجميع المتطلبات (التنوع، النقض، الأمن، الكفاءة). على الرغم من كل هذا، لا تزال تُستخدَم الأنظمة البيومترية (غير المحمية) لتأمين الحدود الدولية، في سيطرة الوصول (Access control) والقضاء على سرقة الهوية!

من خلال جَرْدِنا لمُجمَل المُقارَبات المُقترَحة لحماية أنظمة التحقق من الهوية البيومترية، يمكننا تقسيم هذه الحلول إلى فئتين رئيسيتين (شكل ٢): حلول دفاعِيَة (Palliative) و حلول استِباقِيَة (Preventive). يمكن تقسيم كل فئة إلى نوعين رئيسيين: مُقارَبات عَتادِيَة (Hardware) و مُقارَبات بَرْمجِيَة (Software).



شكل ٢ : نقاط و مستويات الهجوم على نظام بيومتري.

عموما، يتم تصميم الحلول الدفاعِيَة لتجنب وقوع هجمات مباشرة ضد وحدة استشعار الأنظمة البيومترية (انظر هجمات المستوى ١ في الشكل ١). يتمثل الهدف الرئيسي من هذه الفئة من الحلول في التمييز بين السمات البيومترية الحقيقية و السمات المُزوَرة، التي تُعرَض مباشرة على وحدة الاستشعار؛ لتقليل احتمال حدوث توقف في النظام. بالنسبة للمقاربات العَتادِيَة لهذه الفئة من الحلول، يتم عادةً إضافة أجهزة خاصة إلى وحدة الإستشعار لكشف السمات البيومترية المزورة (مثلاً، عن طريق استعمال الخصائص الحرارية). على سبيل المثال لا الحصر، اقترح [Lapslay et al. 1998] جهاز استشعار لبصمات الأصابع يمكنه تحديد ما إذا كان ضغط الدم لسمة بيومترية مُقدَمة يتناسق مع الضغط البشري الطبيعي. كما اقترح [Baldisserra et al. 2005] جهازاً للاستشعار مُطوَراً يسخدم رائحة الجلد للكشف عن البصمات المزورة. يعمل هذا الجهاز و أجهزة أخرى [Franco & Maltoni 2008]، على التقاط الرائحة التي تُخلِفها الجزيئات الصغيرة المُتبخِرة (من المواد الكميائية المُستعملة في محاكاة البصمات) في كشف السمات المزورة. اقترح أيضاً [Pacut & Czajka 2006] جهاز استشعار مطوراً يعتمد على انكماش حدقة العين (Pupil) لكشف القزحية (Iris) المزورة. يستغل هذا الجهاز حساسية الحدقة (وهو ثقب في منتصف القزحية) لتغيرات الإضاءة؛ لأن وظيفة الحدقة هي تنظيم كمية الضوء التي تدخل العين عن طريق تحفيز حركات العضلات المحيطة بالقزحية. حيث تكون هذه الحركات غائبة أو محدودة للغاية في حالة ما إذا كان الخصم يضع قزحية مزورة.

بالنسبة للمقاربات البرمجيةَ التي تندرج في إطار الحلول الرفاعيةَ، فهي تستخدم الميزات المُستخرَجة من صور السمة البومترية التي تبعث بها وحدة الاستشعار إلى وحدة استخراج السمات، و لا تستخدم السمات البيومترية بعينها كما هو الحال في المقاربات العنادية. يتم عادةً استخدام برامج معلوماتية معينة في عملية التقاط و معالجة الصور للتأكد من صدقية السمات البيومترية. على سبيل المثال، يتم في الأعمال [Tai et al. 2006, Yau et al. 2007, Cheng & Larin 2007, Rowe et al. 2008] استغلال الخصائص البصرية الخاصة بجلد الإنسان (مثل الانعكاس والانكسار) لكشف بصمات الأصابع المزورة. حيث تختلف الخصائص البصرية لجلد الإنسان عن تلك الخاصة بالمواد الاصطناعية المُستخدَمة في تصميم البصمات المزورة. في الأعمال [Moon et al. 2005, Choi et al. 2007, Tan & Schuckers 2008]، يتم استغلال الصور ذات دقة تفاصيل عالية (High resolution)، التي توفرها بعض وحدات الاستشعار الحديثة، لاستخدام التفاصيل العميقة من الجلد، كموقع وشكل المسام لكشف البصمات المزورة؛ لأنه يصعب جداً صناعة نماذج مزورة تحتوي على هذه الخصائص المِجْهرية بدقة عالية. تتضمن الأعمال [Pan et al. 2008, Sun et al. 2011] تفاصيل عدة حول حلول عتادية برمجية مُصمَمة خصيصاً لأنظمة التعرف على الوجه. تُمثِل التقنية [Galbally et al. 2012] مثالاً واعداً لكشف القزحية المزورة، كما تمثل الأعمال [Guo et al. 2001, Fierrez & Ortega-Garcia 2008] أمثلةً لتقنيات خاصة بكشف التوقيعات المغشوشة أو المُقلدَة.

تجدر الإشارة إلى أنه في إطار هذه الفئة من الحلول، ليس هنالك تقنية مُوحَدة يمكن تطبيقها على جميع الأنظمة لأن تصميمها يعتمد بالدرجة الأولى على نوع السمة البومترية المُستخدَمة. إضافة إلى هذا، تُعتبَر المقاربات البرمجية أفضل من المقاربات العتادية لكونها أقل تكلفةً بكثير في التطبيقات الواقعية على اعتبار أنها لا تستلزم أي أجهزة إضافية. لكن مع ذلك، لا يزال الجمع بين المقاربات العتادية و البرمجية هو الطريقة الأمثل و الأكثر فعالية لمقاومة أفضل للهجمات المباشرة ضد وحدة الإستشعار.

أما بخصوص الحلول الاسْتباقيةُ (و التي نُوليها اهتماماً أكبرَ في هذه الأطروحة)، فهي تحاول عموماً حماية النماذج البيومترية المُخزَنة في وحدة قاعدة بيانات النظام. تهدف أساساً هذه الفئة من الحلول إلى معالجة مشكلة إلغاء النماذج البيومترية تهدف هذه الفئة من الحلول أساساً إلى معالجة مشكلة إلغاء النماذج البيومترية (انظر الصفحة ١٢٠). تسعى جل المقاربات الاستباقية العنادية إلى نقل ما أمكن من وحدات نظام التحقق إلى أجهزة آمنة (على سبيل المثال، بطاقة ذكية تحتوي على ذاكرة القراءة فقط (ROM)، ذاكرة الوصول العشوائي (RAM)، ذاكرة تخزين و نظام تشغيل بسيط) لضمان أن النماذج البيومترية لا تغادر هذه الأجهزة الآمنة، و بالتالي يتم الحد من هجمات التسلل [Bolle et al. 2002, Cooper et al. 2007] (Intrusion attacks). تَستخدم هذه التقنيات وحدات معالجة مركزية (Processor) خاصة يُمْكنها القيام بعمليات تشفير بسيطة. يمكننا عموماً أن نميز أسلوبين أساسيين من هذه التقنيات: أسلوب Match-on-Card (MoC) و أسلوب System-on-a-Chip (SoC). يَكْمُن الفرق الجوهري بين الأسلوبين في كون البطاقة الذكية في (MoC) تضم فقط وحدة قاعدة البيانات و وحدة التصنيف، بينما يتم إضافة وحدة استخراج السمات أيضاً في البطاقات الذكية الخاصة ب (SoC).

بشكل عام، تتميز المقاربات العتادية بكونها لا تسمح للنماذج البيومترية بمغادرة البطاقة أثناء التشغيل.

لكن بالمقابل، تُعْتبر هذه التكنولوجيا غير مناسبة لمعظم التطبيقات واسعة النطاق، لأنها من جهة مكلفة جداً، ومن جهة أخرى، لأنه يمكن استخراج النماذج البيومترية من بطاقة مسروقة.

أما فيما يخص المقاربات الاستباقية البرمجيةُ، فهي مُصمَمة أساساً لحماية النماذج البيومترية المُخزَنة في قاعدة بيانات النظام. تتمثل الفكرة الأساسية لهذه المقاربات في تخزين نماذج مُحوَلة (بواسطة دالة رياضية أو تحويل هندسي) بدلاً من تخزين النماذج الأصلية في حد ذاتها. يمكننا تصنيف هذه المقاربات البرمجية إلى ثلاث فئات (شكل ٢) [Jain et al. 2008, Rathgeb & Uhl 2011]: مقاربات تحويل السمات، مقاربات التشفير البيومتري و المقاربات الهجينة.

تتمحور الفكرة الأساسية لمقاربات تحويل السمات (Transformation approaches) حول إيجاد دوال رياضية مناسبة لتحويل النماذج غير المحمية إلى أخرى محمية تُستخدَم مباشرة في التصنيف [Ratha et al. 2001]. يُمْكن أن تأخذ دالة التحويل أشكالاً عديدةً، حسب طبيعة النظام و أيضاً حسب نوع السمة البيومترية المُستخدَمة؛ كما يُمْكن أن يتطلب استخدام هذه الدالة وجود معطيات معينة للتحويل (مثلاً، مفتاح المُستخدِم). في حالة سرقة النماذج البيومترية، يتم تعديل معطيات التحويل لتحديثها و جعلها محمية من جديد. لمنع المحتالين من تعقب المستخدمين الشرعيين المسجلين في عدة أنظمة، و من أجل حماية الخصوصية، يجب تطبيق معطيات تحويل مختلفة أو حتى دوال تحويل مختلفة لكل نظام من هذه الأنظمة. تَبَعاً لطبيعة وخصائص دالة التحويل، يمكننا تقسيم مقاربات تحويل السمات إلى فئتين أساسيتين: التحويل المعكوس (Salting or Biohashing) إذا كانت دالة التحويل عكسية و التحويل غير المعكوس (Non-invertible Transformation) إذا كانت دالة التحويل غير عكسية. يُوفِر التحويل المعكوس شروط النقض و التنوع و الكفاءة، بينما يعجز عن توفير الأمن الكافي لأنه إذا تَمَكن الخصم من سرقة نموذج محمي و معطيات تحويله، صار قادراً على استعادة النموذج الأصلي. باختصار، إن تحقيق التوازن بين الأمن و الكفاءة هو التحدي الأكبر أمام تصميم مقاربات التحويل بمختلف أنواعها.

أما في مقاربات التشفير البيومتري (Biometric cryptosystems) [Uludag et al. 2004]، فقد تم الجمع بين مبدأ أنظمة التشفير التقليدية [Schneier 1995, Ferguson et al. 2010] و مبدأ المقاييس الحيوية لتحسين أمن أنظمة التحقق من الهوية. الهدف الرئيسي من هذه المقاربات هو التقليل ما أمكن من كمية السمات البيومترية المُخزَنة في النماذج البيومترية المحمية و في وحدة قاعدة البيانات بشكل عام. وفقاً لمعيار المواصفات ISO/IEC 24745 [ISO/IEC 2011]، فإنه ليس من الواضح دائما كيف تؤثر مقاربات التشفير البيومترية على الكفاءة العامة للأنظمة المحمية من حيث معدلات الرفض الخاطئ و القبول الخاطئ. بالإضافة إلى ذلك، تم إلى حد الآن القيام بعدد قليل من الأعمال لاختبار و دراسة الهجمات المُحتمَلة ضد أنظمة التشفير البيومترية، مما يجعل سلامتها و مدى أمنها غير معروف الى حد كبير. في الآونة الأخيرة، أظهرت بعض الدراسات، مثل [Blanton & Aliasgari 2013]، أن هذا النوع من المقاربات لا يزال عرضة لعدد من الهجمات، وأنه لا يمكن إعادة استخدامها بأمان إذا سبق و تعرضت فعلاً لانتهاك أمني ما.

عندما يتم في تقنية ما لحماية النماذج البيومترية الإستناد إلى أكثر من مقاربة من المقاربات الأساسية (سواء من تحويل السمات أو التشفير البيومتري)؛ يطلق عليها اسم المقاربة الهجينة (Hybrid approach).

أهداف ومساهمات الأطروحة

تتمثل الأهداف الرئيسية للأطروحة فيما يلي:

(١). دراسة شاملة لمشكل أمن أنظمة التحقق من الهوية البيومترية لتحديد وتقييم التهديدات والهجمات المُحتمَلة مع التركيز على تلك المُتعلِقة بالنماذج البيومترية.

(٢). دراسة و تحليل شامل لجل الحلول الحالية المُقترَحة لتعزيز أمن أنظمة التحقق من الهوية البيومترية مع التركيز على مقاربات حماية النماذج البيومترية.

(٣). تطوير مقاربات جديدة لحماية النماذج البيومترية لتحسين أمن و مقاومة أنظمة التحقق من الهوية البيومترية ضد الهجمات المحتملة دون تغيير جذري في بنية و وحدات الأنظمة المحمية.

(٤). تقييم المقاربات المُقترَحة باستخدام بروتوكولات فعالة وقواعد بيانات اختبار مُتاحة على نطاق واسع لكل الباحثين في هذا المجال.

تَكْمُن المساهمات الرئيسية التي تقدمها الأطروحة فيما يلي:

(١). تصميم مقاربة جديدة، تنتمي إلى مقاربات تحويل السمات غير المعكوسة، تعتمد على الإسقاط العشوائي (Random Projection)، تم تسميتها المكعب اللولبي (Spiral Cube)، لحماية النماذج البيومترية المُمثَلة على شكل متجهات، تستجيب لمتطلبات النقض، التنوع، الأمن و الكفاءة. تم استخدام تحليل صارم ودقيق و كذا تجارب مكثفة و واسعة النطاق على أربع قواعد بيانات و ثلاث سمات بيومترية لتقييم المقاربة المُقترَحة. كما تم مقارنة المكعب اللولبي مع اثنين من مقاربات الحماية التي تستند أيضاً على استخدام الإسقاط العشوائي.

(٢). تصميم مقاربة جديدة، تنتمي إلى مقاربات تحويل السمات غير المعكوسة، لحماية أنظمة التعرف على بصمات الأصابع، و التي تستخدم نماذج بيومترية مُمثَلةً على شكل تفصيلات (Minutiae). لقد تم اقترح نموذج أو تمثيل محمي جديد، يُدعى قوقعة البصمة (Fingerprint Shell)، والذي يُمْكن استخدامه بدلاً من التمثيل التقليدي القائم على التفصيلات. إضافة إلى كون أن هذه المقارنة الجديدة تلبي جميع المتطلبات الأربعة للتقنيات المثالية، فهي أيضاً أقل تأثراً بدوران و إزاحة بصمات الأصابع في وحدة الإستشعار (بالمقارنة مع العديد من مقاربات الحماية)، كما أنها قوية بما يكفي ضد هجمات المجهود المنعدم و هجمات القوة العمياء.

نريد أن نؤكد في نهاية هذه الملخص، أن الأمن المطلق غير موجود. و لعله من المهم جدا أيضاً أن نفهم ببساطة أنه لا وجود لأنظمة تحقق من الهوية (سواء تقليدية أو بيومترية) مثالية؛ وربما لن يكون لها وجود أبداً. لكن بالمقابل، يمكننا أن نؤكد على أنه بإمكاننا الوثوق بأمن أنظمة التحقق البيومترية إذا ما اسْتُخدِمت بحذر وبالتزامن مع تقنيات حماية أخرى.

ANNEXE A

Annexes

A.1 L'algorithme Hill-Climbing

Pour régénérer les images originales à partir les scores de correspondance, l'algorithme Hill-Climbing fonctionne comme suit [Adler 2003] :

- On teste plusieurs images dans le système et on collecte les scores de correspondance. L'image I_i qui a le plus grand score S_i est utilisée comme une image d'attaque initiale.
- On va modifier I_i sur plusieurs itératives pour construire l'estimation finale I_f comme suit :
  1. Modifier aléatoirement I_i.
  2. Calculer le score S_f en utilisant l'image modifiée.
  3. Si $S_f > S_i$, Alors $I_i = I_f$ et $S_i = S_f$
  4. Arrêter l'algorithme si S_f ne s'augmente plus.

Le défi majeur dans l'implémentation de cet algorithme d'attaque, est de trouver la faÃ§on optimale ou logique pour modifier I_i de telle manière S_f s'augmente.

A.2 Orthogonalisation de Gram-Schmidt

Soit v_1, v_2, ... , v_n un ensemble de vecteurs linéairement indépendants. L'orthogonalisation de Gram-Schmidt fonctionne comme suit :

$$u_1 = v_1 \; et \; u_1 \frac{u_1}{\|u_1\|} \tag{A.1}$$

$$u_2 = v_2 - proj_{u_1} v_2 \; et \; u_2 \frac{u_2}{\|u_2\|} \tag{A.2}$$

$$u_i = v_i - \sum_{k=1}^{i} -1 proj_{u_k} v_i \; et \; u_i \frac{u_i}{\|u_i\|} \tag{A.3}$$

– $proj$ est l'opérateur de projection orthogonale
– $proj_u v = \langle u, v \rangle u$

– $\langle u, v \rangle$ est le produit scalaire.
– $\|.\|$ la norme d'un vecteur.

A.3 Régénération d'un modèle protégé par BioPhasor

Si nous avons un modèle biométrique t protégé par BioPhasor, Nous appliquons les équations (3.3) et (3.4) sut t (avec $\tau = \pi$) pour calculer l'approximation $\tilde{z}$ (voir page 46) ; et nous proposons d'ajouter cette étape d'optimisation sur $\tilde{z}$ comme suit :

$$\hat{z}_i = \Delta_{i1} \times tan\left(m\tilde{z}_1 - \sum_{j=2}^{m} atan\left(\frac{1}{\Delta_{ij} \times \tilde{z}_j}\right)\right) \tag{A.4}$$

– $m \leq n$ et $i = 1,\ldots,n$.
– $\hat{z}$ il est l'approximation finale pour un modèle BioPhasor.

A.4 Laplacian Smoothing Transform (LST)

Dans ce travail, nous avons utilisé la technique LST, vu qu'elle a prouvé sa robustesse par rapport aux approches fréquentielles actuelles [Gu *et al.* 2010, Moujahdi *et al.* 2014b], de plus elle conserve la liaison entre les pixels. La plupart des approches fréquentielles utilisées souffrent du problème de la complexité calculatoire (2 heures pour calculer les vecteurs propres des images de taille 64×64). Pour la LST, la complexité du calcul réside essentiellement dans le nombre de vecteurs propres minimaux de la matrice Laplacienne LMN à calculer pour des images de taille M $\times$ N. Heureusement, L_{MN} est une matrice creuse, elle peut être calculée rapidement et une seule fois pour la formation (10 secondes pour calculer les 200 premiers vecteurs propres de $L_{100,100}$). LST a comme but de passer du domaine spatial d'une image à son domaine fréquentiel. Ainsi les hautes fréquences de l'image (contenant le bruit par exemple) peuvent être supprimées tout en gardant les données majeures qui sont représentées par les basses fréquences, et tout en gardant la liaison entre les pixels. Les étapes principales de LST sont :

– Calculer la matrice de poids W de taille $MN \times MN$ (M et N sont les dimensions de l'images) :

$$W\left(\lceil x,y \rceil \lceil x',y' \rceil\right) = \begin{cases} 1 & \text{if } |x-x'|+|y-y'| = 1 \\ 0 & \text{if } |x-x'|+|y-y'| \neq 1 \end{cases} \tag{A.5}$$

  – $\lceil x,y \rceil = x \times N + y$
  – x et y sont les coordonnées du pixel.

– Calculer la matrice diagonale D :

$$D(\lceil x,y\rceil\lceil x,y\rceil) = \sum_{\lceil x,y\rceil} W\left(\lceil x,y\rceil\lceil x^{'},y^{'}\rceil\right) \tag{A.6}$$

– Calculer la matrice laplacienne L_{MN} :

$$L_{MN} = D - W \tag{A.7}$$

– Calculer les k premières valeurs propres et ses k vecteurs propres correspondants E_k (k dépend du nombre de basses fréquences voulues).
– Projeter les images de formation et de test en utilisant E_k.

A.5 Algorithme de construction d'une courbe F.S

Algorithm 1 Fingerprint Curve construction

Input : Sorted distances $d_1\ d_2\ ...\ d_n$ of a fingerprint impression
Parameters : User's key d_0
Output : A fingerprint curve FC
Let $DIS = [d_0,\ d_1+d_0,\ d_2+d_0,\ ...,\ d_n+d_0]$ and $\theta_1 = 0$
for $i = 1$ to $n+1$ **do**
  if $i == 1$ **then**
    $Leg_i = \sqrt{DIS_{i+1}^2 - d_0^2}$ ▷ Leg distance of the first right triangle
    $x = [0\ DIS_i\ DIS_i\ 0]$ ▷ Points abscissae of the first triangle
    $y = [0\ 0\ Leg_i\ 0]$ ▷ Points ordinates of the first triangle
  end if
  if $i > 1$ **then**
    $Leg_i = \sqrt{DIS_{i+1}^2 - DIS_i^2}$ ▷ Leg distance of the next right triangle
    $\theta_i = -atan\left(\frac{Leg_{i-1}}{DIS_{i-1}}\right)$
    $\theta_i = \theta_i + \theta_{i-1}$ ▷ Angle between d_0 and the last constructed leg
    $x = [0\ DIS_i\ DIS_i\ 0]$
    $y = [0\ 0\ Leg_i\ 0]$
    for $j = 1$ to 4 **do**
      $\Upsilon = [x_j\ y_j] \times \begin{bmatrix} cos(\theta_i) & -sin(\theta_i) \\ sin(\theta_i) & cos(\theta_i) \end{bmatrix}$ ▷ Change of basis
      $x_j = \Upsilon_1$ and $y_j = \Upsilon_2$ ▷ Coordinates in the vector space frame of the first triangle
    end for
  end if
  $CurveX_i = x_3$ and $CurveY_i = y_3$
end for
$FC(1,:) = CurveX$ ▷ Points abscissae of the fingerprint curve
$FC(2,:) = CurveY$ ▷ Points ordinates of the fingerprint curve

Bibliographie

[Achlioptas 2003] Dimitris Achlioptas. *Database-friendly Random Projections : Johnson-Lindenstrauss with Binary Coins*. Journal of Computer and System Sciences, vol. 66, no. 4, pages 671–687, Juin 2003. (Cité en page 114.)

[Adler & Schuckers 2007] A. Adler et M.E. Schuckers. *Comparing Human and Automatic Face Recognition Performance*. Systems, Man, and Cybernetics, Part B : Cybernetics, IEEE Transactions on, vol. 37, no. 5, pages 1248–1255, 2007. (Cité en page 57.)

[Adler 2003] A. Adler. *Sample images can be independently restored from face recognition templates*. In IEEE Canadian Conference on Electrical and Computer Engineering, volume 2, pages 1163–1166 vol.2, 2003. (Cité en pages 1, 28, 29, 33 et 127.)

[Adler 2004] A. Adler. *Images can be regenerated from quantized biometric match score data*. In IEEE Canadian Conference on Electrical and Computer Engineering, 2004, volume 1, pages 469–472, 2004. (Cité en pages 24 et 32.)

[Adler 2005] A. Adler. *Vulnerabilities in Biometric Encryption Systems*. In Audio- and Video-Based Biometric Person Authentication, volume 3546, pages 1100–1109. Springer Berlin Heidelberg, 2005. (Cité en pages 10, 24 et 28.)

[Ahmad *et al.* 2011] Tohari Ahmad, Jiankun Hu et Song Wang. *Pair-polar Coordinate-based Cancelable Fingerprint Templates*. Pattern Recognition, vol. 44, no. 10-11, pages 2555–2564, 2011. (Cité en page 101.)

[Ahn *et al.* 2008] Dosung Ahn, S.G. Kong, Yun-Su Chung et Ki Young Moon. *Matching with Secure Fingerprint Templates Using Non-invertible Transform*. In Image and Signal Processing, 2008. CISP '08. Congress on, volume 2, pages 29–33, 2008. (Cité en pages 101 et 108.)

[Albrecht *et al.* 2003] A. Albrecht, M. Behrens, T. Mansfield, W. McMeechan, M. R. Greene, M. Savastano, P. Statham, C. Schmidt, B. Schouten et M. Walsh. *BioVision : Roadmap for Biometrics In Europe to 2010*. CWI : REPORT PNA-E0303, 2003. (Cité en pages 21 et 33.)

[Alonso-Fernandez *et al.* 2009] F. Alonso-Fernandez, J. Fierrez, A. Gilperez, J. Galbally et J. Ortega-Garcia. *Robustness of Signature Verification Systems to Imitators with Increasing Skills*. In Document Analysis and Recognition, 2009. ICDAR '09. 10th International Conference on, pages 728–732, 2009. (Cité en page 25.)

[Antonelli *et al.* 2006] A. Antonelli, R. Cappelli, D. Maio et D. Maltoni. *Fake finger detection by skin distortion analysis*. Information Forensics and Security, IEEE Transactions on, vol. 1, no. 3, pages 360–373, 2006. (Cité en page 26.)

[Arakala *et al.* 2007] Arathi Arakala, Jason Jeffers et K. J. Horadam. *Fuzzy Extractors for Minutiae-based Fingerprint Authentication*. In Proceedings of the 2007 International Conference on Advances in Biometrics, pages 760–769, Berlin, Heidelberg, 2007. Springer-Verlag. (Cité en page 54.)

[Argones Rua *et al.* 2012] E. Argones Rua, E. Maiorana, J.L. Alba Castro et P. Campisi. *Biometric Template Protection Using Universal Background Models : An Application to Online Signature*. Information Forensics and Security, IEEE Transactions on, vol. 7, no. 1, pages 269–282, 2012. (Cité en page 53.)

[Baldisserra *et al.* 2005] Denis Baldisserra, Annalisa Franco, Dario Maio et Davide Maltoni. *Fake Fingerprint Detection by Odor Analysis*. In Advances in Biometrics, volume 3832 of *Lecture Notes in Computer Science*, pages 265–272. Springer Berlin Heidelberg, 2005. (Cité en page 39.)

[Bhatnagar & Wu 2012] G. Bhatnagar et Q. M J Wu. *Chaos-Based Security Solution for Fingerprint Data During Communication and Transmission*. Instrumentation and Measurement, IEEE Transactions on, vol. 61, no. 4, pages 876–887, 2012. (Cité en page 72.)

[Blanton & Aliasgari 2013] M. Blanton et M. Aliasgari. *Analysis of Reusability of Secure Sketches and Fuzzy Extractors*. Information Forensics and Security, IEEE Transactions on, vol. 8, no. 9, pages 1433–1445, 2013. (Cité en pages 54 et 55.)

[Bolle *et al.* 2002] Ruud M. Bolle, Jonathan H. Connell et Nalini K. Ratha. *Biometric perils and patches*. Pattern Recognition, vol. 35, no. 12, pages 2727 – 2738, 2002. (Cité en pages 28, 41 et 47.)

[Boult *et al.* 2007] T.E. Boult, W.J. Scheirer et R. Woodworth. *Revocable fingerprint biotokens : accuracy and security analysis*. In IEEE Conference on Computer Vision and Pattern Recognition, 2007. CVPR '07, pages 1–8, 2007. (Cité en pages 50, 56 et 108.)

[Breebaart *et al.* 2009] J. Breebaart, B. Yang, I. B. Dulman et C. Busch. *Biometric Template Protection : The need for open standards*. Privacy and Data Security journal, 2009. (Cité en pages 22 et 35.)

[Bringer *et al.* 2008] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji et G. Zemor. *Theoretical and Practical Boundaries of Binary Secure Sketches*. IEEE Transactions on Information Forensics and Security, vol. 3, no. 4, pages 673–683, 2008. (Cité en page 54.)

[Campisi 2013] P. Campisi. Security and privacy in biometrics. Springer Publishing Company, Incorporated, 2013. (Cité en pages 1, 21, 22, 35, 43, 46, 48 et 49.)

[Cappelli *et al.* 2006] R. Cappelli, D. Maio, D. Maltoni, J.L. Wayman et A.K. Jain. *Performance evaluation of fingerprint verification systems*. Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 28, no. 1, pages 3–18, 2006. (Cité en pages 58 et 64.)

[Cappelli *et al.* 2007] R. Cappelli, D. Maio, A. Lumini et D. Maltoni. *Fingerprint Image Reconstruction from Standard Templates*. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 9, pages 1489–1503, 2007. (Cité en pages 97 et 100.)

[Cappelli *et al.* 2010] R. Cappelli, M. Ferrara et D. Maltoni. *Minutia Cylinder-Code : A New Representation and Matching Technique for Fingerprint Recognition*. Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 32, no. 12, pages 2128–2141, 2010. (Cité en page 101.)

[Chang *et al.* 2004] Yao-Jen Chang, Wende Zhang et Tsuhan Chen. *Biometrics-based cryptographic key generation*. In Multimedia and Expo, 2004. ICME '04. 2004 IEEE International Conference on, volume 3, pages 2203–2206, 2004. (Cité en page 54.)

[Cheng & Larin 2007] Yezeng Cheng et K.V. Larin. *In Vivo Two- and Three-Dimensional Imaging of Artificial and Real Fingerprints With Optical Coherence Tomography*. Photonics Technology Letters, IEEE, vol. 19, no. 20, pages 1634–1636, 2007. (Cité en page 40.)

[Chikkerur *et al.* 2008] S. Chikkerur, N.K. Ratha, J.H. Connell et R.M. Bolle. *Generating Registration-free Cancelable Fingerprint Templates*. In 2nd IEEE International Conference on Biometrics : Theory, Applications and Systems, 2008. BTAS 2008., pages 1–6, 2008. (Cité en page 51.)

[Chin *et al.* 2006] Chong Siew Chin, Andrew Teoh Beng Jin et David Ngo Chek Ling. *High security Iris verification system based on random secret integration*. Comput. Vis. Image Underst., vol. 102, no. 2, pages 169–177, Mai 2006. (Cité en page 46.)

[Choi *et al.* 2007] H. Choi, R. Kang, K. Choi et J. Kim. *Aliveness Detection of Fingerprints using Multiple Static Features*. International Journal of Biomedical Science, vol. 2, no. 3, pages 200–205, 2007. (Cité en page 40.)

[Connie *et al.* 2005] Tee Connie, Andrew Teoh, Michael Goh et David Ngo. *PalmHashing : a novel approach for cancelable biometrics*. Information Processing Letters, vol. 93, no. 1, pages 1–5, Janvier 2005. (Cité en page 46.)

[Cooper *et al.* 2007] D. Cooper, H. Dang, P. Lee, W. MacGregor et K. Mehta. *Secure Biometric Match-on-Card Feasibility Report*. NIST Interagency Report 7452, 2007. (Cité en pages 31 et 41.)

[Cukic & Bartlow 2005] B. Cukic et N. Bartlow. *Biometric System Threats and Countermeasures : A Risk Based Approach*. In Biometric Consortium Conference, 2005. (Cité en pages 10 et 24.)

[Daugman 2004] J. Daugman. *How iris recognition works*. Circuits and Systems for Video Technology, IEEE Transactions on, vol. 14, no. 1, pages 21–30, 2004. (Cité en page 89.)

[Dodis *et al.* 2008] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin et Adam Smith. *Fuzzy Extractors : How to Generate Strong Keys from Biometrics and Other Noisy Data*. SIAM Journal on Computing, vol. 38, no. 1, pages 97–139, Mars 2008. (Cité en page 54.)

[El-Abed 2006] Mohamad El-Abed. *Evaluation de systèmes biométriques*. PhD thesis, Ecole doctorale S.I.M.E.M, Université de Caen Basse-Normandie, Aout 2006. (Cité en page 62.)

[Eriksson & Wretling 1997] Anders Eriksson et Pär Wretling. *How flexible is the human voice ? - a case study of mimicry*. In Fifth European Conference on Speech Communication and Technology, EUROSPEECH 1997, Rhodes, Greece, September 22-25, 1997. ISCA, 1997. (Cité en page 25.)

[Farooq *et al.* 2007] F. Farooq, R.M. Bolle, Tsai-Yang Jea et N. Ratha. *Anonymous and Revocable Fingerprint Recognition*. In Computer Vision and Pattern Recognition, 2007. CVPR '07. IEEE Conference on, pages 1–7, 2007. (Cité en page 101.)

[Feng & Wah 2002] Hao Feng et Chan Choong Wah. *Private key generation from on-line handwritten signatures*. Information Management & Computer Security, vol. 10, no. 4, pages 159–164, 2002. (Cité en page 54.)

[Feng *et al.* 2010] Y. C. Feng, P.C. Yuen et A.K. Jain. *A Hybrid Approach for Generating Secure and Discriminating Face Template*. IEEE Transactions on Information Forensics and Security, vol. 5, no. 1, pages 103–117, 2010. (Cité en page 55.)

[Ferguson *et al.* 2010] N. Ferguson, B. Schneier et T. Kohno. *Cryptography Engineering*. John Wiley & Sons, 2010. (Cité en pages 8, 18 et 51.)

[Ferrara *et al.* 2012] M. Ferrara, D. Maltoni et R. Cappelli. *Noninvertible Minutia Cylinder-Code Representation*. IEEE Transactions on Information Forensics and Security, vol. 7, no. 6, pages 1727–1737, 2012. (Cité en pages 51, 101 et 108.)

[Fierrez & Ortega-Garcia 2008] Julian Fierrez et Javier Ortega-Garcia. *On-Line Signature Verification*. In AnilK. Jain, Patrick Flynn et ArunA. Ross, editeurs, Handbook of Biometrics, pages 189–209. Springer US, 2008. (Cité en page 40.)

[Franco & Maltoni 2008] Annalisa Franco et Davide Maltoni. *Fingerprint Synthesis and Spoof Detection*. In Advances in Biometrics, pages 385–406. Springer London, 2008. (Cité en pages 27 et 39.)

[Galbally *et al.* 2009] J. Galbally, F. Alonso-Fernandez, J. Fierrez et J. Ortega-Garcia. *Fingerprint Liveness Detection Based on Quality Measures*. In IEEE Proc. Intl. Conf. on Biometrics, Identity and Security, BIDS, September 2009. (Cité en page 26.)

[Galbally *et al.* 2010] J. Galbally, R. Cappelli, A. Lumini, G. Gonzalez de Rivera, D. Maltoni, J. Fierrez, J. Ortega-Garcia et D. Maio. *An Evaluation of Direct Attacks Using Fake Fingers Generated from ISO Templates*. Pattern Recognition Letters, vol. 31, no. 8, pages 725–732, June 2010. (Cité en pages 1, 25, 33, 97 et 100.)

[Galbally *et al.* 2012] J. Galbally, J. Ortiz-Lopez, J. Fierrez et J. Ortega-Garcia. *Iris liveness detection based on quality related features*. In Biometrics (ICB), 2012 5th IAPR International Conference on, pages 271–276, 2012. (Cité en page 40.)

[Geradts 2006] Zeno Geradts. *Forensic implications of identity systems*. Datenschutz und Datensicherheit - DuD, vol. 30, no. 9, pages 557–559, 2006. (Cité en page 25.)

[Goel *et al.* 2005] Navin Goel, George Bebis et Ara Nefian. *Face recognition experiments with random projection*, 2005. (Cité en page 44.)

[Goutis & Robert 1998] C. Goutis et C. P. Robert. *Model choice in generalised linear models : A Bayesian approach via Kullback-Leibler projections*. Biometrika, vol. 85, pages 29–37, 1998. (Cité en page 102.)

[Grother *et al.* 2009] P. Grother, W. Salamon, C. Watson, M. Indovina, et P. Flanagan. *Performance of Fingerprint Match-on-Card Algorithms Phase II / III Report*. NIST Interagency Report 7477 (Revision I), 2009. (Cité en page 31.)

[Gu *et al.* 2010] SuiCheng Gu, Ying Tan et XinGui He. *Laplacian smoothing transform for face recognition*. Science China Information Sciences, vol. 53, no. 12, pages 2415–2428, 2010. (Cité en pages 79 et 128.)

[Guo *et al.* 2001] J. K. Guo, D.Doermann et A. Rosenfeld. *Forgery Detection by Local Correspondence*. International Journal of Pattern Recognition and Artificial Intelligence, vol. 15, no. 04, pages 579–641, 2001. (Cité en page 40.)

[Hao *et al.* 2006] Feng Hao, R. Anderson et J. Daugman. *Combining Cryptography with Biometrics Effectively*. IEEE Transactions on Computers, vol. 55, no. 9, pages 1081–1088, 2006. (Cité en pages 52 et 53.)

[Hämmerle-Uhl *et al.* 2009] Jutta Hämmerle-Uhl, Elias Pschernig et Andreas Uhl. *Cancelable Iris Biometrics Using Block Re-mapping and Image Warping*. In Pierangela Samarati, Moti Yung, Fabio Martinelli et ClaudioA. Ardagna, editeurs, Information Security, volume 5735 of *Lecture Notes in Computer Science*, pages 135–142. Springer Berlin Heidelberg, 2009. (Cité en page 50.)

[Holland & Komogortsev 2013] C.D. Holland et O.V. Komogortsev. *Complex eye movement pattern biometrics : Analyzing fixations and saccades*. In Biometrics (ICB), 2013 International Conference on, pages 1–8, 2013. (Cité en pages 63 et 67.)

[INCITS 2006] INCITS. *InterNational Committee for Information Technology Standards : Study report on biometrics in e-authentication*. Technical Report INCITS M1/06-0693, 2006. (Cité en page 21.)

[ISO/IEC 2011] ISO/IEC. *Information technology – Security techniques – Biometric information protection*. ISO/IEC 24745 :2011(E), 2011. (Cité en pages 11, 33, 35 et 55.)

[Jain *et al.* 2006] A.K. Jain, A. Ross et S. Pankanti. *Biometrics : a tool for information security*. Information Forensics and Security, IEEE Transactions on, vol. 1, no. 2, pages 125–143, 2006. (Cité en pages 10 et 24.)

[Jain *et al.* 2007] A. K. Jain, P. Flynn et A. A. Ross. Handbook of biometrics. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007. (Cité en pages 21, 33 et 47.)

[Jain *et al.* 2008] A. k. Jain, K. Nandakumar et A. Nagar. *Biometric Template Security*. EURASIP Journal on Advances in Signal Processing, no. 1, pages 1–17, 2008. (Cité en pages 1, 2, 10, 23, 24, 35, 41, 43, 44, 47, 48, 51, 52, 54 et 101.)

[Jin *et al.* 2004] Andrew Teoh Beng Jin, David Ngo Chek Ling et Alwyn Goh. *Biohashing : two factor authentication featuring fingerprint data and tokenised random number*. Pattern Recognition, vol. 37, no. 11, pages 2245–2255, 2004. (Cité en pages 45 et 46.)

[Juels & Sudan 2002] A. Juels et M. Sudan. *A fuzzy vault scheme*. In Proceedings of IEEE International Symposium on Information Theory., pages 408–, 2002. (Cité en pages 52 et 53.)

[Juels & Wattenberg 1999] Ari Juels et Martin Wattenberg. *A fuzzy commitment scheme*. In Proceedings of the 6th ACM conference on Computer and communications security, CCS '99, pages 28–36, New York, NY, USA, 1999. ACM. (Cité en pages 52 et 53.)

[Juels *et al.* 2005] A. Juels, D. Molnar et D. Wagner. *Security and Privacy Issues in E-passports*. In Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on, pages 74–88, 2005. (Cité en page 28.)

[Kappraff *et al.* 2005] Jay Kappraff, Slavik Jablan, Gary Adamson et Radmila Sazdanovich. *Golden Fields, Generalized Fibonacci Sequences, and Chaotic Matrices*. In Reza Sarhangi et Robert V. Moody, editeurs, Renaissance Banff : Mathematics, Music, Art, Culture, pages 369–378. Canadian Mathematical Society, 2005. (Cité en page 72.)

[Kerckhoffs 1883] A. Kerckhoffs. *La cryptographie militaire*. Journal des sciences militaires, pages 5–38, 1883. (Cité en page 22.)

[Kholmatov & Yanikoglu 2006] Alisher Kholmatov et Berrin Yanikoglu. *Biometric Cryptosystem Using Online Signatures*. In Computer and Information Sciences, volume 4263 of *Lecture Notes in Computer Science*, pages 981–990. Springer Berlin Heidelberg, 2006. (Cité en page 53.)

[Kim *et al.* 2013] Sooyeon Kim, Sunjin Yu, Kwangtaek Kim, Yuseok Ban et Sangyoun Lee. *Face liveness detection using variable focusing*. In Biometrics (ICB), 2013 International Conference on, pages 1–6, 2013. (Cité en page 26.)

[Kong *et al.* 2006] Adams Kong, King-Hong Cheung, David Zhang, Mohamed Kamel et Jane You. *An analysis of BioHashing and its variants*. Pattern Recognition, vol. 39, no. 7, pages 1359–1368, Juillet 2006. (Cité en page 46.)

[Kryszczuk *et al.* 2004] KrzysztofM. Kryszczuk, Patrice Morier et Andrzej Drygajlo. *Study of the Distinctiveness of Level 2 and Level 3 Features in Fragmentary Fingerprint Comparison*. In Davide Maltoni et AnilK. Jain, editeurs, Biometric Authentication, volume 3087 of *Lecture Notes in Computer Science*, pages 124–133. Springer Berlin Heidelberg, 2004. (Cité en pages 2 et 99.)

[Kumar & Kumar 2008] Amioy Kumar et Ajay Kumar. *A palmprint-based cryptosystem using double encryption*, 2008. (Cité en page 54.)

[Kumar *et al.* 2010] G. Kumar, S. Tulyakov et V. Govindaraju. *Combination of Symmetric Hash Functions for Secure Fingerprint Matching*. In Pattern Recognition (ICPR), 2010 20th International Conference on, pages 890–893, 2010. (Cité en pages 101 et 108.)

[Lam & Beth 1992] Kwok-Yan Lam et Thomas Beth. *Timely authentication in distributed systems*. In Computer Security, volume 648 of *Lecture Notes in Computer Science*, pages 293 – 303. Springer Berlin Heidelberg, 1992. (Cité en page 28.)

[Lapslay *et al.* 1998] P. D. Lapslay, J. A. Lee, D. F. Pare et N. Hoffman. *Anti-Fraud Biometric Scanner That Accurately Detects Blood Flow*. United States Patent Number 5737439, 1998. (Cité en page 39.)

[Lee *et al.* 2005] EuiChul Lee, KangRyoung Park et Jaihie Kim. *Fake Iris Detection by Using Purkinje Image*. In Advances in Biometrics, volume 3832 of *Lecture Notes*

in Computer Science, pages 397–403. Springer Berlin Heidelberg, 2005. (Cité en page 26.)

[Lee *et al.* 2007] Chulhan Lee, Jeung-Yoon Choi, Kar-Ann Toh et Sangyoun Lee. *Alignment-Free Cancelable Fingerprint Templates Based on Local Minutiae Information*. IEEE transactions on systems man and cybernetics - Part b, vol. 37, no. 4, pages 980–992, Août 2007. (Cité en pages 51 et 63.)

[Lewis & Statham 2004] M. Lewis et P. Statham. *CESG biometric security capabilities programme : method, results and research challenges*, 2004. (Cité en page 25.)

[Li & Kot 2012] Sheng Li et A.C. Kot. *An Improved Scheme for Full Fingerprint Reconstruction*. IEEE Transactions on Information Forensics and Security, vol. 7, no. 6, pages 1906–1912, 2012. (Cité en pages 97 et 100.)

[Li *et al.* 2008] Qiming Li, Muchuan Guo et E.-C. Chang. *Fuzzy extractors for asymmetric biometric representations*. In Computer Vision and Pattern Recognition Workshops, 2008. CVPRW '08. IEEE Computer Society Conference on, pages 1–6, 2008. (Cité en page 54.)

[Li *et al.* 2010] Peng Li, Xin Yang, Kai Cao, Xunqiang Tao, Ruifang Wang et Jie Tian. *An alignment-free fingerprint cryptosystem based on fuzzy vault scheme*. Journal of Network and Computer Applications, vol. 33, no. 3, pages 207–220, 2010. (Cité en pages 53 et 101.)

[Lu *et al.* 2009] Haiping Lu, K. Martin, F. Bui, K.N. Plataniotis et D. Hatzinakos. *Face recognition with biometric encryption for privacy-enhancing self-exclusion*. In Digital Signal Processing, 2009 16th International Conference on, pages 1–8, 2009. (Cité en page 53.)

[Maio *et al.* 2002] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman et A.K. Jain. *FVC2000 : fingerprint verification competition*. Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 24, no. 3, pages 402–412, 2002. (Cité en pages 58, 60, 63, 64 et 105.)

[Maiorana & Campisi 2010] E. Maiorana et P. Campisi. *Fuzzy Commitment for Function Based Signature Template Protection*. Signal Processing Letters, IEEE, vol. 17, no. 3, pages 249–252, 2010. (Cité en page 53.)

[Maiorana *et al.* 2008a] E. Maiorana, P. Campisi, J. Ortega-Garcia et A. Neri. *Cancelable Biometrics for HMM-based Signature Recognition*. In Biometrics : Theory, Applications and Systems, 2008. BTAS 2008. 2nd IEEE International Conference on, pages 1–6, 2008. (Cité en page 51.)

[Maiorana *et al.* 2008b] E. Maiorana, M. Martinez-Diaz, P. Campisi, J. Ortega-Garcia et A. Neri. *Template protection for HMM-based on-line signature authentication*. In

Computer Vision and Pattern Recognition Workshops, 2008. CVPRW '08. IEEE Computer Society Conference on, pages 1–6, 2008. (Cité en page 51.)

[Maiorana *et al.* 2010] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia et A. Neri. *Cancelable Templates for Sequence-Based Biometrics with Application to On-line Signature Recognition*. Systems, Man and Cybernetics, Part A : Systems and Humans, IEEE Transactions on, vol. 40, no. 3, pages 525–538, 2010. (Cité en pages 50 et 51.)

[Maltoni *et al.* 2003] D. Maltoni, D. Maio, A. k. Jain et S. Prabhakar. Handbook of fingerprint recognition. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2003. (Cité en pages 18, 31, 47, 58, 100 et 102.)

[Maltoni *et al.* 2009] Davide Maltoni, Dario Maio, Anil K. Jain et Salil Prabhakar. Handbook of fingerprint recognition. Springer Publishing Company, Incorporated, 2nd édition, 2009. (Cité en pages 97, 100 et 102.)

[Manneville 2005] Paul Manneville. *Dynamique non linéaire et chaos*. In Séminaire E2PHY Pôle Scientifique de Paris-Sud, 2005. (Cité en page 72.)

[Masek & Kovesi 2003] L. Masek et P. Kovesi. *Matlab Source Code for a Biometric Identification System Based on Iris Patterns*. The School of Computer Science and Software Engineering, The University of Western Australia, 2003. (Cité en pages 2, 78 et 79.)

[Matsumoto *et al.* 2002] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada et Satoshi Hoshino. *Impact of artificial "gummy" fingers on fingerprint systems*, 2002. (Cité en page 25.)

[Monrose *et al.* 2001] Fabian Monrose, Michael K. Reiter, Qi Li et Susanne Wetzel. *Cryptographic Key Generation from Voice*. In Proceedings of the 2001 IEEE Symposium on Security and Privacy, SP '01, Washington, DC, USA, 2001. IEEE Computer Society. (Cité en page 54.)

[Moon *et al.* 2005] Y.S. Moon, J.S. Chen, K. C. Chan, K. So et K. C. Woo. *Wavelet based fingerprint liveness detection*. Electronics Letters, vol. 41, no. 20, pages 1112–1113, 2005. (Cité en page 40.)

[Moujahdi *et al.* 2012] Chouaib Moujahdi, Sanaa Ghouzali, Mounia Mikram, Mohammed Rziza et George Bebis. *Spiral Cube for Biometric Template Protection*. In Image and Signal Processing, volume 7340 of *Lecture Notes in Computer Science*, pages 235–244. Springer Berlin Heidelberg, 2012. (Cité en pages 70, 97 et 100.)

[Moujahdi *et al.* 2014a] Chouaib Moujahdi, George Bebis, Sanaa Ghouzali et Mohammed Rziza. *Fingerprint shell : Secure representation of fingerprint template*. Pattern Recognition Letters, vol. 45, no. 0, pages 189 – 196, 2014. (Cité en page 70.)

[Moujahdi *et al.* 2014b] Chouaib Moujahdi, Sanaa Ghouzali, Mounia Mikram, Abdul Wadood et Mohammed Rziza. *Inter-Communication Classification for Multi-View Face Recognition*. The International Arab Journal of Information Technology, vol. 11, no. 4, 2014. (Cité en page 128.)

[Nagar *et al.* 2010] Abhishek Nagar, Karthik Nandakumar et Anil K. Jain. *Biometric template transformation : a security analysis.* In Media Forensics and Security, volume 7541 of *SPIE Proceedings*. SPIE, 2010. (Cité en pages 1, 45, 46, 49, 57, 58 et 65.)

[Nandakumar *et al.* 2007a] K. Nandakumar, A.K. Jain et S. Pankanti. *Fingerprint-Based Fuzzy Vault : Implementation and Performance*. Information Forensics and Security, IEEE Transactions on, vol. 2, no. 4, pages 744–757, 2007. (Cité en page 53.)

[Nandakumar *et al.* 2007b] Karthik Nandakumar, Abhishek Nagar et Anil K. Jain. *Hardening Fingerprint Fuzzy Vault Using Password.* In Proceedings of the 2007 International Conference on Advances in Biometrics, pages 927–937, Berlin, Heidelberg, 2007. Springer-Verlag. (Cité en page 56.)

[Nandakumar 2010] K. Nandakumar. *A fingerprint cryptosystem based on minutiae phase spectrum*. In IEEE International Workshop on Information Forensics and Security (WIFS), pages 1–6, 2010. (Cité en page 53.)

[Nguyen *et al.* 2013] T.H. Nguyen, Y. Wang, Y. Ha et R. Li. *Improved chaff point generation for vault scheme in bio-cryptosystems*. Biometrics, IET, vol. 2, no. 2, pages 48–55, 2013. (Cité en page 53.)

[Pacut & Czajka 2006] A. Pacut et A. Czajka. *Aliveness Detection for IRIS Biometrics*. In Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International, pages 122–129, 2006. (Cité en page 39.)

[Pan *et al.* 2008] Gang Pan, Zhaohui Wu et Lin Sun. *Recent Advances in Face Recognition*. Capter Liveness Detection for Face Recognition, 2008. (Cité en page 40.)

[Pankanti *et al.* 2002] S. Pankanti, S. Prabhakar et A.K. Jain. *On the individuality of fingerprints*. Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 24, no. 8, pages 1010–1025, 2002. (Cité en page 24.)

[Parthasaradhi *et al.* 2005] S.T.V. Parthasaradhi, R. Derakhshani, L.A. Hornak et S. A C Schuckers. *Time-series detection of perspiration as a liveness test in fingerprint devices*. Systems, Man, and Cybernetics, Part C : Applications and Reviews, IEEE Transactions on, vol. 35, no. 3, pages 335–343, 2005. (Cité en page 26.)

[Pillai *et al.* 2010] J.K. Pillai, V.M. Patel, R. Chellappa et N.K. Ratha. *Sectored Random Projections for Cancelable Iris Biometrics*. In Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on, pages 1838–1841, 2010. (Cité en page 44.)

[Pillai *et al.* 2011] Jaishanker K. Pillai, Vishal M. Patel, Rama Chellappa et Nalini K. Ratha. *Secure and Robust Iris Recognition Using Random Projections and Sparse Representations*. IEEE Trans. Pattern Anal. Mach. Intell., vol. 33, no. 9, pages 1877–1893, Septembre 2011. (Cité en page 46.)

[Quan *et al.* 2008] Feng Quan, Su Fei, Cai Anni et Zhao Feifei. *Cracking Cancelable Fingerprint Template of Ratha*. In Computer Science and Computational Technology, 2008. ISCSCT '08. International Symposium on, volume 2, pages 572–575, 2008. (Cité en page 50.)

[Rane *et al.* 2013] S. Rane, Ye Wang, S.C. Draper et P. Ishwar. *Secure Biometrics : Concepts, Authentication Architectures, and Challenges*. Signal Processing Magazine, IEEE, vol. 30, no. 5, pages 51–64, 2013. (Cité en pages 1, 48 et 49.)

[Ratha *et al.* 2001] N. K. Ratha, J. H. Connell et R. M. Bolle. *Enhancing security and privacy in biometrics-based authentication systems*. IBM Systems Journal, vol. 40, no. 3, pages 614–634, 2001. (Cité en pages 10, 12, 24, 35, 43 et 47.)

[Ratha *et al.* 2003] N. K. Ratha, J. H. Connell et R. M. Bolle. *Biometrics break-ins and band-aids*. Pattern Recognition Letters, vol. 24, no. 13, pages 2105 – 2113, 2003. (Cité en pages 10 et 24.)

[Ratha *et al.* 2006] N. K. Ratha, J. H. Connell, R. M. Bolle et S. Chikkerur. *Cancelable Biometrics : A Case Study in Fingerprints*. In Pattern Recognition, 2006. ICPR 2006. 18th International Conference on, volume 4, pages 370–373, 2006. (Cité en pages 7, 33, 43, 47 et 49.)

[Ratha *et al.* 2007] N.K. Ratha, S. Chikkerur, J.H. Connell et R.M. Bolle. *Generating Cancelable Fingerprint Templates*. Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 29, no. 4, pages 561–572, 2007. (Cité en pages 47, 49, 97 et 101.)

[Rathgeb & Uhl 2010a] C. Rathgeb et A. Uhl. *Adaptive fuzzy commitment scheme based on iris-code error analysis*. In Visual Information Processing (EUVIP), 2010 2nd European Workshop on, pages 41–44, 2010. (Cité en page 53.)

[Rathgeb & Uhl 2010b] Christian Rathgeb et Andreas Uhl. *Privacy Preserving Key Generation for Iris Biometrics*. In Proceedings of the 11th IFIP TC 6/TC 11 International Conference on Communications and Multimedia Security, CMS'10, pages 191–200, Berlin, Heidelberg, 2010. Springer-Verlag. (Cité en page 55.)

[Rathgeb & Uhl 2010c] Christian Rathgeb et Andreas Uhl. *Secure Iris Recognition Based on Local Intensity Variations*. In Aurélio Campilho et Mohamed Kamel, editeurs, Image Analysis and Recognition, volume 6112 of *Lecture Notes in Computer Science*, pages 266–275. Springer Berlin Heidelberg, 2010. (Cité en page 50.)

[Rathgeb & Uhl 2011] Christian Rathgeb et Andreas Uhl. *A survey on biometric cryptosystems and cancelable biometrics*. EURASIP Journal on Information Security, vol. 2011, no. 1, pages 1–25, 2011. (Cité en pages 41, 43, 44, 47, 48 et 52.)

[Roberts 2007] C. Roberts. *Biometric attack vectors and defences*. Computers & Security, vol. 26, no. 1, pages 14–25, 2007. (Cité en pages 10 et 24.)

[Ross *et al.* 2005] Arun A. Ross, Jidnya Shah et Anil K. Jain. *Toward reconstructing fingerprints from minutiae points*, 2005. (Cité en page 97.)

[Ross *et al.* 2007] Arun Ross, Jidnya Shah et Anil K. Jain. *From Template to Image : Reconstructing Fingerprints from Minutiae Points*. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pages 544–560, Avril 2007. (Cité en pages 97 et 100.)

[Rowe *et al.* 2008] RobertK. Rowe, KristinAdair Nixon et PaulW. Butler. *Multispectral Fingerprint Image Acquisition*. In Advances in Biometrics, pages 3–23. Springer London, 2008. (Cité en pages 27 et 40.)

[Sakata *et al.* 2006] Koji Sakata, Takuji Maeda, Masahito Matsushita, Koichi Sasakawa et Hisashi Tamaki. *Fingerprint authentication based on matching scores with other data*. In Proceedings of the 2006 international conference on Advances in Biometrics, ICB'06, pages 280–286, Berlin, Heidelberg, 2006. Springer-Verlag. (Cité en page 46.)

[Savvides *et al.* 2004] M. Savvides, B.V.K.V. Kumar et P.K. Khosla. *Cancelable biometric filters for face recognition*. In Proceedings of the 17th International Conference on Pattern Recognition, volume 3, pages 922–925 Vol.3, 2004. (Cité en page 46.)

[Schneier 1995] Bruce Schneier. Applied cryptography (2nd ed.) : protocols, algorithms, and source code in c. John Wiley & Sons, Inc., New York, NY, USA, 1995. (Cité en pages 28 et 51.)

[Schuckers 2002] Stephanie A. C. Schuckers. *Spoofing and anti-spoofing measures*. Information Security Technical Report, vol. 7, pages 56–62, 2002. (Cité en page 24.)

[Song *et al.* 2008] Ong Thian Song, Andrew Teoh, Beng Jin, David Chek, Ling Ngo et Corresponding Ong Thian. *Application-Specific Key Release Scheme from Biometrics*. International Journal of Network Security, pages 127–133, 2008. (Cité en page 56.)

[Soutar 2002] C. Soutar. *Biometric System Security*. Secure : The Silicon Trust Magazine, pages 46–49, 2002. (Cité en pages 28 et 29.)

[Sun *et al.* 2011] Lin Sun, WaiBin Huang et MingHui Wu. *TIR/VIS correlation for liveness detection in face recognition*. In Proceedings of the 14th international confe-

rence on Computer analysis of images and patterns - Volume Part II, CAIP'11, pages 114–121, Berlin, Heidelberg, 2011. Springer-Verlag. (Cité en page 40.)

[Sutcu *et al.* 2005] Yagiz Sutcu, Husrev Taha Sencar et Nasir Memon. *A Secure Biometric Authentication Scheme Based on Robust Hashing*. In Proceedings of the 7th Workshop on Multimedia and Security, pages 111–116, New York, NY, USA, 2005. (Cité en page 50.)

[Sutcu *et al.* 2007] Yagiz Sutcu, Qiming Li et N. Memon. *Protecting Biometric Templates With Sketch : Theory and Practice*. Trans. Info. For. Sec., vol. 2, no. 3, pages 503–512, Septembre 2007. (Cité en page 54.)

[Syverson 1994] P. Syverson. *A taxonomy of replay attacks [cryptographic protocols]*. In Computer Security Foundations Workshop VII, 1994. CSFW 7. Proceedings, pages 187–191, 1994. (Cité en pages 24 et 28.)

[Tai *et al.* 2006] Katsuki Tai, Masashi Kurita et Ichiro Fujieda. *Recognition of living fingers with a sensor based on scattered-light detection*. Appl. Opt., vol. 45, no. 3, pages 419–424, Jan 2006. (Cité en page 40.)

[Tan & Schuckers 2008] Bozhao Tan et Stephanie A. C. Schuckers. *New approach for liveness detection in fingerprint scanners based on valley noise analysis*. J. Electronic Imaging, vol. 17, no. 1, page 011009, 2008. (Cité en page 40.)

[Teoh & Ong 2008] A. Teoh et Thian-Song Ong. *Secure biometric template protection via randomized dynamic quantization transformation*. In Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium on, pages 1–6, 2008. (Cité en page 53.)

[Teoh *et al.* 2006] A.B.J. Teoh, A. Goh et D.C.L. Ngo. *Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs*. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 28, no. 12, pages 1892–1901, 2006. (Cité en page 46.)

[Teoh *et al.* 2007] Andrew Beng Jin Teoh, Kar-Ann Toh et Wai Kuan Yip. 2^N *discretisation of biophasor in cancellable biometrics*. In Proceedings of the 2007 international conference on Advances in Biometrics, ICB'07, pages 435–444, Berlin, Heidelberg, 2007. Springer-Verlag. (Cité en pages 48, 50 et 100.)

[Tulyakov *et al.* 2007] Sergey Tulyakov, Faisal Farooq, Praveer Mansukhani et Venu Govindaraju. *Symmetric Hash Functions for Secure Fingerprint Biometric Systems*. Pattern Recognition Letters, vol. 28, no. 16, pages 2427–2436, 2007. (Cité en pages 101 et 108.)

[Uludag & Jain 2004] Umut Uludag et Anil K. Jain. *Attacks on Biometric Systems : A Case Study in Fingerprints*. In Proc. SPIE-EI 2004, Security, Seganography and Watermarking of Multimedia Contents VI, pages 622–633, 2004. (Cité en page 28.)

[Uludag *et al.* 2004] U. Uludag, S. Pankanti, S. Prabhakar et A.K. Jain. *Biometric cryptosystems : issues and challenges*. Proceedings of the IEEE, vol. 92, no. 6, pages 948–960, 2004. (Cité en page 51.)

[Uz *et al.* 2009] Tamer Uz, George Bebis, Ali Erol et Salil Prabhakar. *Minutiae-based Template Synthesis and Matching for Fingerprint Authentication*. Comput. Vis. Image Underst., vol. 113, no. 9, pages 979–992, Septembre 2009. (Cité en pages 2 et 101.)

[Veen *et al.* 2006] Michiel Van Der Veen, Tom Kevenaar, Geert jan Schrijen, Ton H. Akkermans, Fei Zuo et Prof Holstlaan. *Face Biometrics with Renewable Templates*. In Proceedings of SPIE, Volume 6072 : Security, Steganography, and Watermarking of Multimedia Contents VIII, Edward J. Delp III, Ping Wah Wong, Editors, 60720J, 2006. (Cité en page 53.)

[Vielhauer *et al.* 2002] C. Vielhauer, R. Steinmetz et A. Mayerhofer. *Biometric hash based on statistical features of online signatures*. In 16th International Conference on Pattern Recognition, volume 1, pages 123–126, 2002. (Cité en page 54.)

[Voderhobli *et al.* 2006] Kiran Voderhobli, Dr. Colin Pattinson et Dr. Helen Donelan. *A schema for cryptographic keys generation using hybrid biometrics*. In 7th annual postgraduate symposium : The convergence of telecommunications, networking and broadcasting, 2006. (Cité en page 56.)

[Wang & Plataniotis 2007] Yongjin Wang et K.N. Plataniotis. *Face Based Biometric Authentication with Changeable and Privacy Preservable Templates*. In Biometrics Symposium, pages 1–6, 2007. (Cité en page 45.)

[Wu *et al.* 2008] Xiangqian Wu, Ning Qi, Kuanquan Wang et David Zhang. *A Novel Cryptosystem Based on Iris Key Generation*. In Proceedings of the 2008 Fourth International Conference on Natural Computation - Volume 04, ICNC '08, pages 53–56, Washington, DC, USA, 2008. IEEE Computer Society. (Cité en page 54.)

[Yang *et al.* 2009] Bian Yang, C. Busch, P. Bours et D. Gafurov. *Non-invertible geometrical transformation for fingerprint minutiae template protection*. In Security and Communication Networks (IWSCN), 2009 Proceedings of the 1st International Workshop on, pages 1–7, 2009. (Cité en page 101.)

[Yang *et al.* 2012] Wencheng Yang, Jiankun Hu et Song Wang. *A Delaunay Triangle-Based Fuzzy Extractor for Fingerprint Authentication*. In IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pages 66–70, 2012. (Cité en page 54.)

[Yau *et al.* 2007] Wei-Yun Yau, Hoang-Thanh Tran, Eam-Khwang Teoh et Jian-Gang Wang. *Fake Finger Detection by Finger Color Change Analysis*. In Seong-Whan

Lee et StanZ. Li, editeurs, Advances in Biometrics, volume 4642 of *Lecture Notes in Computer Science*, pages 888–896. Springer Berlin Heidelberg, 2007. (Cité en page 40.)

[Zhang *et al.* 2013] Lijia Zhang, Bo Liu, Xiangjun Xin, Qi Zhang, Jianjun Yu et Yongjun Wang. *Theory and Performance Analyses in Secure CO-OFDM Transmission System Based on Two-Dimensional Permutation*. Lightwave Technology, Journal of, vol. 31, no. 1, pages 74–80, 2013. (Cité en page 72.)

[Zhou 2007] Xuebing Zhou. *Template protection and its implementation in 3D face recognition systems*, 2007. (Cité en page 54.)

[Zuo *et al.* 2008] Jinyu Zuo, N.K. Ratha et J.H. Connell. *Cancelable Iris Biometric*. In Pattern Recognition, 2008. ICPR 2008. 19th International Conference on, pages 1–4, 2008. (Cité en page 50.)